UNIVERSIDADE DE LISBOA

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE INFORMÁTICA

Cloud Security Risk and Readiness

Luís Paulo Teixeira Ferreira

Mestrado em Segurança Informática

Dissertação orientada por:
Professora Doutora Ana Luísa do Carmo Correia Respício
Mestre Sérgio Valentim Costa de Sá

2017

Acknowledgments

First, I would like to thank Prof. Ana Respicio for her guidance throughout this thesis, helping me being more pragmatic in order to overcome the coexistence challenge of my academic and professional life. I must also mention the professors I encountered during the three years at FCUL. Each one contributed to the success of my academic and professional path.

I express my gratitude to Eng. Sergio Sá for his availability and willingness to be part of this work, as well as for the increased value provided. Also, I would like to appreciate the important contribution given by: Eng. Alessandra Rodrigues, Eng. Pedro Dias Rodrigues and Eng. Daniel Caçador.

To my friends from FCUL, who were also immensely supportive throughout this journey, namely Pedro Chaves, Raimundo and Sergio. I highlight Pedro Chaves, as he was my companion through long studying weekends and nights at FCUL, providing not only support but also, more importantly, the unwinding moments that made me carry on.

For all the patience, support, love and friendship demonstrated during this journey, I thank you Rita. I have no words to describe how grateful I am to have you as girlfriend.

Last but not least, I am grateful for having my parents' unconditional support throughout this academic journey, as well as from my brother (and his wife) and sister.

Dedicated to My girlfriend, My father and My grandfather Serafim.

Resumo

Num mundo cada vez mais dependente da informação trocada através de meios digitais, é visível a evolução do paradigma das soluções informáticas tradicionais para o tema emergente, e cada vez mais convincente, da Computação em Nuvem. Tal facto deve-se não só às características diferenciadoras deste tipo de estrutura (e.g. on-demand self-service, ubiquidade, rápida elasticidade, flexibilidade, entre outros) e à maior eficácia na gestão e utilização de recursos de TI, mas também, de um ponto de vista empresarial, aos benefícios comerciais inerentes, como contenção de despesas (capitais e/ou operacionais), que se enquadram perfeitamente nas constantes mudanças das necessidades de negócio das organizações. Um conceito chave relativamente a esta matéria é o facto dos clientes conseguirem, de um modo geral, reduzir custos em recursos como licenciamento de software, hardware ou até outros serviços como o email, visto que conseguem usufruir de toda uma panóplia de serviços do mesmo fornecedor.

A Computação na Nuvem é um modelo de computação que permite o acesso a um conjunto partilhado de recursos computacionais configuráveis (e.g. Rede, servidores, aplicações e serviços) de uma forma ubíqua e conveniente, sendo que estes recursos podem ser rapidamente aprovisionados e desaprovisionados sem encargos de gestão relevantes assim como sem interação com o fornecedor de serviço. De forma mais ampla, o paradigma da Computação em Nuvem parte do princípio de que todos os recursos de infraestrutura de tecnologias de informação (hardware, software e gestão de dados e informação), até então tratados como ativos pelas organizações que os utilizam, passam a ser alojados numa infraestrutura dum fornecedor de tecnologia como um serviço (ou fornecedor de serviços tecnológicos) e acedidos e administrados por estas através da internet com o uso de um simples browser web. A Computação em Nuvem fornece uma camada de abstração entre os recursos de computação e a arquitetura de baixo nível que se encontra subjacente. Esta camada de abstração é um argumento muito atraente para organizações que apenas se querem focar nos recursos relevantes para o seu negócio sem necessitarem de fazer investimentos avultados em infraestrutura física e recursos humanos internos para gerir essa mesma infraestrutura. Ou seja, nos dias que correm, os clientes podem apenas fazer subscrições de serviços com fornecedores de Computação em Nuvem, o que lhes concede acesso aos mesmos recursos e infraestrutura, no entanto de uma forma mais imediata e alinhada com as condições e necessidades de negócio (em constante mutação). Este modelo de computação "as-a-service" tem alterado drasticamente a forma de atuar das organizações, tal como a forma como os departamentos de informática dessas mesmas organizações obtêm recursos computacionais e de armazenamento para garantir um elevado indice de escalabilidade. No entanto, à medida que mais organizações movem dados e infraestrutura para a Nuvem, a segurança vai-se revelando cada vez mais um tópico de especial relevância. De uma forma genérica, muitos fornecedores de Computação em Nuvem não transmitem aos seus clientes a transparência necessária relativamente aos controlos de segurança que utilizam para mitigar os eventuais riscos e ameaças de segurança inerentes a estes ambientes (em parte devido ao elevado grau de exposição dos serviços em Nuvem relativamente à Internet). Neste contexto,

o modelo de Computação em Nuvem reveste-se de particularidades que o distinguem dos tradicionais modelos de computação, na medida em que os riscos são diferentes para cada modelo de serviço na Nuvem (IaaS, PaaS, SaaS) assim como para cada modelo de implementação (Privada, Pública, Comunitária, Híbrida). Por outro lado, os clientes também não estão devidamente preparados para esta realidade, de um ponto de vista de segurança e de adaptação do modelo de governo, para utilizar estes serviços. O nível global de segurança de uma organização é caracterizado pela maturidade dos controlos implementados para mitigar o risco. Estes controlos são implementados em várias camadas, desde a segurança física, segurança de redes, segurança de recursos humanos, até à segurança da informação e das aplicações (segurança aplicacional).

Nos ambientes de Computação em Nuvem as responsabilidades dos consumidores pelos vários domínios de segurança e respetivos controlos variam consoante o modelo de serviço utilizado. Se uma determinada entidade está a considerar utilizar algum tipo de serviço de Computação em Nuvem, esta deveria aferir os riscos associados ao(s) modelo(s) de serviço/implementação aplicáveis e, consequentemente, identificar casos de uso que representem um nível de risco aceitável para assim poder avançar para a adoção deste modelo computacional em Nuvem. Todavia, devido aos requisitos de imediatismo (geralmente impostos pelos executivos das organizações) relacionados com as necessidades de negócio, a análise e avaliação de riscos (assim como a sua mitigação) é, de um modo geral, negligenciada pelas equipas internas (de informática e segurança) aquando de uma migração de ativos de informação para a Nuvem. Embora este mercado esteja a crescer, apesar dos potenciais problemas de segurança adjacentes, a projeção da taxa de crescimento relativa ao consumo de serviços em Nuvem poderia ser maior se as organizações começassem a implementar processos internos mais adequados para a avaliação do seu grau de maturidade ao nível dos controlos de segurança aplicáveis em ambientes de Computação na Nuvem. Esta avaliação permitiria uma melhor gestão de risco relativamente à segurança de dados, assim como a identificação de possíveis melhorias em áreas específicas de segurança. Essas melhorias depois de implementadas traduzem-se em mais confiança e motivação das organizações para usufruir das vantagens da Computação em Nuvem. De salientar que este tipo de análise e avaliação de maturidade e riscos por parte de consumidores, tendo em conta os diferentes fornecedores de serviços em Nuvem, devem ser balanceados com uma revisão dos possíveis benefícios de escala provenientes deste modelo, especificamente em termos de segurança (e.g. Mais meios de deteção de anomalias, assim como melhor capacidade de resposta a incidentes de segurança). A Computação em Nuvem tem um potencial significante para melhorar a segurança e resiliência de organizações que não possuem um nível de maturidade de segurança satisfatório tendo em conta essas áreas.

Tendo em conta os tópicos abordados, o autor do presente trabalho acredita que existia a necessidade de criação de uma metodologia que, não só suportasse a tomada de decisão das organizações relativamente à implementação de mecanismos apropriados de gestão e mitigação de risco, mas que também permitisse aferir o nível de maturidade de segurança em Nuvem de uma forma holística, ou seja, cobrindo de um modo geral as diversas áreas de

segurança mais relevantes. Esta dissertação propõe uma abordagem que, através de um modelo de avaliação de maturidade, permitirá aos clientes de serviços em Nuvem responder às necessidades já mencionadas no âmbito das diversas áreas de segurança (como conformidade ou proteção de dados). Este modelo também incorpora componentes que permitem a identificação de potenciais fatores de risco resultantes da utilização dos diferentes modelos de serviço e implementação da Computação em Nuvem. O modelo criado é traduzido da teoria para a prática através dum protótipo desenvolvido pelo autor. Além das funcionalidades de avaliação do nível de maturidade de segurança em Nuvem e identificação de possíveis fatores de risco, o protótipo também fornece dashboards que contêm informações relevantes sobre os resultados da avaliação. Os resultados obtidos devem permitir que uma organização compare diferentes fornecedores de serviços de Computação em Nuvem, ajudando desta forma a tomada de decisão por parte dos quadros superiores, assim como negoceie de uma forma mais consciente e fundamentada os acordos de nível de serviço (SLAs) com os fornecedores, obtendo desta forma algum tipo de garantias de segurança por parte dos mesmos. Uma primeira avaliação realizada por especialistas nas áreas de Computação em Nuvem e segurança revelou que o protótipo é uma contribuição importante para as avaliações de segurança em Nuvem, assim como tem aplicabilidade em ambientes organizacionais com requisitos de segurança e compliance elevados.

Palavras-chave: Segurança, Nuvem, Risco, *Assessment*, *Readiness*

Abstract

Within the "Information Era", the world has become increasingly dependent on information exchanged through digital media and it is clear that the paradigm of traditional IT solutions is evolving rapidly to emerging areas (and more and more convincing) like Cloud Computing. This is due not only to the differentiating characteristics of Cloud Computing services (e.g. *on-demand self-service*, ubiquity, rapid elasticity, flexibility, among others) and to the greater effectiveness in the management and use of IT resources, but also, from a business point of view, it is due to the inherent commercial benefits, such as cost containment (both capital and operational costs), which fit perfectly into the constantly changing business needs of organizations. Although the advantages of using Cloud Computing services are easily identified from a business point of view, many potential consumers are reluctant to use these services to host their information assets due to the fact that, at least at the first stage, they will have to deal with the unknown (their being used to traditional computing environments), as well as due to the risks and security threats inherent to these environments resulting from the high degree of exposure to the Internet. In this context, the Cloud Computing model has particularities that distinguish it from the traditional computing models insofar as the risks are different for each service model in the Cloud (IaaS, PaaS, SaaS) as well as for each implementation model (Private, Public, Community, Hybrid). Based on that, there is a need for a methodology which, from an IT and information security perspective, not only supports the decision-making of the organizations that consume cloud services with regards to the implementation of appropriate risk management and mitigation mechanisms, but also which enables the organizations to assess its maturity level regarding the implemented controls (that will help mitigate cloud security risks) and, consequently, the forecasting of security areas that should be improved. This, in turn, helps the organizations to achieve a satisfactory mature state that enables the use of cloud services in a more proper and secure way ("security readiness").

This dissertation proposes a holistic approach which, through a designed assessment model, will enable Cloud services customers to tackle the aforementioned needs across several different security areas (such as compliance, governance or data protection), as well as will allow the identification of potential risk factors related with the use of Cloud Computing. This theoretical model is translated into practise through a prototype tool developed by the author. Apart from the Cloud security maturity assessment and potential risk factors identification functionalities, the prototype also provides dashboards that give valuable insights about the assessment results. A first evaluation performed by experts in the cloud and security fields revealed that the prototype is an important contribution for Cloud Security assessments in organizational environments.

Keywords: Security, Cloud, Risk, Assessment, Readiness

Content

List of Figures

List of Tables

Chapter 1 Introduction

Within the “Information Era”, the world has become increasingly dependent on information exchanged through digital media and it is clear that the paradigm of traditional IT solutions is evolving rapidly to emerging areas (and more and more convincing) like Cloud Computing. This is due not only to the characteristics of Cloud Computing services (e.g. *on-demand self-service,* ubiquity, rapid elasticity, and flexibility, among others) and to the greater effectiveness in the management and use of IT resources, but also, from a business point of view, to the inherent commercial benefits, such as cost containment (both capital and operational costs), which fit perfectly into the constantly changing business needs of organizations.

Although the advantages of using Cloud Computing services are easily identified from a business point of view (in that it facilitates business activities and increases productivity and profitability), many potential consumers are reluctant to use these services to host their information assets due to the fact that, at least at the first stage, they will have to deal with the unknown (as they are used to traditional computing environments), as well as due to the risks and security threats inherent to these environments resulting from the high degree of exposure to the Internet (making the company more vulnerable and more exposed to external attackers). In this context, organizations should have specific Cloud security controls in place to mitigate Cloud specific risks, because the Cloud Computing model has particularities which distinguish it from the traditional computing models insofar as the risks are different for each service model in the "Cloud" (IaaS, PaaS, SaaS) as well as for each implementation model (Private, Public, Community, Hybrid).

1.1 Motivation

This dissertation responds to a gap in the existence of models (e.g. computational tools) that enable the assessment of cloud security maturity level (in terms of controls implemented) of the organizations which use Cloud services or intend to migrate services to it, as well as risk evaluation regarding the use of Cloud Computing solutions. In addition to the Informatics Department of the Faculty of Sciences of the Lisbon University (FCUL), this work relies on a collaboration of EY Portugal, a company which provides information security consulting services to national and international markets. This synergy between the security business market and the academic environment is an excellent opportunity because it enables both the identification of the organization's security needs (mostly in the Portuguese security market) as well as a scientific approach to addressing those needs. In the specific context of this project, the objective was to marry the spheres of business and academia, producing an academic work with business relevance.

The project is directly linked to the several services provided through Cloud Computing, a paradigm which has emerged with special relevance in the IT market and which, according to experts in the field, has had a notable growth with increasing adoption by organizations from different industries worldwide. The main reason for such growth is the need for organizations' IT teams to respond to business requirements, both in terms of cost reduction and also with regards to ubiquity, efficiency, and immediacy. However, due to these requirements and needs (usually imposed by the organization's senior management), the analysis and evaluation of security-related risks and prior mitigation is often neglected by IT teams when moving information assets to the Cloud. Although this market is growing in spite of the potential security issues, the growth rate projection of Cloud services could be much higher if organizations started putting into practice appropriate security maturity evaluation and risk analysis processes to identify the security domains that need improvement and to identify and mitigate cloud security risks.

If a particular entity or organization is considering the use of any Cloud Computing service, it should:

- Assess operational, privacy, governance and compliance risks;
- Classify its assets and identify inappropriate use cases for the cloud computing service delivery model, based on the level of risk and currently implemented controls (maturity level);
- Identify use cases that represent an acceptable level of risk for the Cloud service delivery model;
- Choose and implement risk compensation controls prior to adopting Cloud Computing services;

In other words, there is a need for a method which, from an IT and information security point of view, not only supports the decision-making of the organizations that consume services regarding the aforementioned points, but also which allows the organizations to assess its maturity level regarding the implemented controls that will help mitigate cloud risks and, consequently, forecast areas that should be improved, enabling the organization to be more mature to use cloud services in a more proper and secure way ("security readiness").

This led to an interest in the design of a maturity level and potential risk assessment model specific for Cloud Computing environments that can allow organizations to respond to some of the problems identified above and to identify what should be improved to achieve readiness levels (from an Information Security point of view) and, consequently, to use Cloud Computing services more securely. The designed maturity assessment model is intended to help an organization analyze the maturity state of its cloud security controls and to define a target state within the context of its business and security goals, and then to perform a gap analysis between its current maturity state and target readiness states.

In other words, after a maturity assessment is completed through the use of the developed tool, an organization should be able to evaluate its degree of cloud security maturity in several different strategic domains (in line with the industry standards) such as compliance, governance and interoperability, enabling a more precise and reasoned definition of the top priority controls that should be implemented to mitigate potential cloud risks and to improve its overall maturity level.

1.2 Objectives

Based essentially on the Information Security topic, the main goal of this work is to help potential Cloud Computing consumers to:

- Through an assessment process, assess the Cloud security maturity level regarding the implementation of controls aimed at mitigating cloud security risks from different security domains and to prioritize the missing controls according the organization's pre-defined target readiness states to be achieved for each domain.
- Evaluate the potential risk factors of using Cloud computing services. For example, the consumers should be able to compare the potential risks of maintaining a classic IT architecture within the organization premises to the risks of using a (third-party) Cloud Computing environment. These potential risks can be mapped (in terms of applicability) to the different Cloud computing service and deployment models, enabling the organization to identify the potential risks according to a specific model they are using or intend to use (e.g. SaaS, Hybrid Cloud).

1.3 Contributions

With the work described in the present document, a model was designed, constituting a starting point in the security maturity assessment paradigm for Cloud Computing environments. This effort is a foundation for future work which may improve the existing model as well as the features of the solution created to that model.

In addition to the research work carried out throughout this process, the most evident result of this work is the prototype which has been built. The prototype tool developed enables organizations to assess their security maturity level regarding Cloud Computing and to identify potential risk factors specific for each Cloud service/deployment model. Furthermore, it allows organizations to define an improvements roadmap regarding Cloud Computing security controls in a more grounded way, thus enabling the organization to clearly identify what is needed to reach the target Cloud security readiness level.

Summing up, the author believes the developed solution prototype work is an important contribution since it enables the cloud service customer to:

- Compare different providers of Cloud Computing services, based on their needs, thereby helping senior management decision-making.
- Identify security requirements to achieve a readiness level regarding the use of Cloud computing services. Thus, enabling the CSC to develop a more balanced cloud strategy.
- Negotiate contracts and service level agreements (SLAs) with cloud providers in a more grounded and informed manner, thus obtaining security guarantees on their side.
- Identify controls that need to be implemented in order to achieve compliance with Industry standards and regulations (e.g. ISO/IEC 27017:2015).
- Understand the dimensions that constitute cloud security maturity.
- Identify an improvements roadmap to accomplish the changes in maturity levels for each security domain.
- Develop focused investment initiatives to reach target maturity levels in relevant cloud security domains, in order to improve their overall security maturity.
- Steer priorities relating to secure cloud service use and adoption.
- Compare different departments and entities from different industries regarding Cloud Security maturity (Benchmarking).

1.4 Document Structure

The present chapter outlines the motivation for the development of this dissertation and, consequently, the objectives which the work intends to meet.

The remainder of this document is structured as follows:

- **Chapter 2 – Context** - The "Context" - initially presents concepts of Cloud Computing as well as its architecture layout. Then, it addresses the relationship between Cloud computing and Security followed by a presentation of the possible Cloud Computing security benefits by highlighting how the use of Cloud Computing services can also be a way of improving overall security for many organizations.

- **Chapter 3 – Related Work** - The chapter "Related Work" succinctly presents the work that was collected and analyzed in order to enrich our knowledge regarding the project. Also, major security risks associated with Cloud Computing are presented, framing the same with the project carried out.

- **Chapter 4 – A solution to assess the security readiness and potential risks on Cloud environments** - The solution is outlined, in terms of the architecture

which was chosen and the various components that make it up (modeling design decisions and the developed prototype features).

- **Chapter 5 – Tool evaluation** - The evaluation process performed to the developed prototype is demonstrated in terms of its utility, usability, and applicability to the real world. Also, an analysis of the results obtained is presented.

- **Chapter 6 – Conclusions and Future** Work - The work and conclusions that can be drawn from it is described, the content and the results presented are discussed and the authors give a perspective on what future work may arise from it.

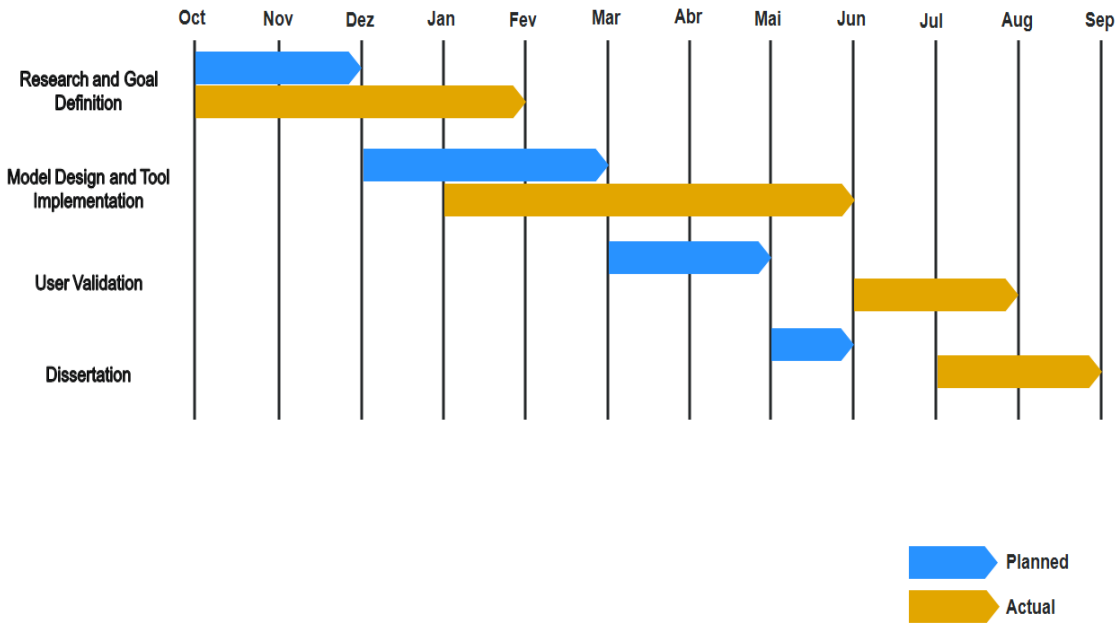
1.5 Project Plan

The project described in this dissertation was developed over a period of eleven months, with sequential stages which built upon previous activities to achieve a coherent outcome.

Although there were no major changes to the project initial planning phases, generally, the different phases consumed more time than was anticipated, starting with the goal definition and finishing with the dissertation.

Figure 1 presents the various stages that made up the project development plan, from the initial research and goal definition to dissertation writing, including model design and tool implementation as well as the resulting User Validation.

Figure 1 - Project Planning and Implementation



Chapter 2 Context

This chapter introduces the Cloud Computing concepts that are essential to understanding the proposed solution as well as the decisions taken in its construction. The chapter starts by explaining what Cloud Computing is, as well as how it differentiates from traditional IT environments. Next, some statistics related with Cloud Computing adoption throughout the past years are presented. Following that, the chapter gives some context regarding the relationship between security and the different Cloud models. Finally, to support the idea that Cloud Computing has significant potential to improve the security of its consumers, potential Cloud security benefits are presented.

2.1 What is Cloud Computing?

Cloud Computing is the result of the evolution and the technical foundations gathering of areas such as server virtualization, among others. It is a flexible and efficient model for using software as well as for storing and processing data through different devices and web technologies.

More broadly, the Cloud Computing paradigm assumes that all IT infrastructure resources (hardware, software and data and information management), which until now have been treated as on-site assets by the organizations who use them, are now housed in third-party provider premises which provide technology as a service (or technological services), as well as accessed and managed by them through the Internet using a simple web browser.

Cloud computing is a computing model that allows access to a shared set of configurable computing resources (e.g. Network, servers, applications, and services) in a ubiquitous and convenient way, with the remark that these resources can be quickly provisioned and de-provisioned without relevant management (operational) effort as well as without interaction with the service provider. This model has specific characteristics which set it apart from "classic" models, three service models and four implementation models. (Mell & Grance, 2011).

It is important to highlight that, for the purpose of this dissertation, the different service and implementation models and related risks should be considered.

2.1.1 Cloud Service Models

Understanding the inter-relationships between different service models of Cloud Computing is essential to understand the underlying security risks. Infrastructure as a Service (IaaS) is the basis of all Cloud services, with Platform as a Service (PaaS) built

upon IaaS, and Software as a Service (SaaS) built on top of PaaS. In this manner, just as resources are inherited, so are the security risks associated with each model.

As described in Table 1, Cloud Computing environments can be composed of three different service models that define their architecture. (Mell & Grance, 2011).

Table 1- Cloud Computing Service Models. Adapted from (Mell & Grance, 2011).

Cloud Service Models	
Model	**Description**
Software as a Service (SaaS)	In this model, the consumer uses applications that run on the cloud service provider infrastructure. The applications are accessible through the internet by using several different devices and their interfaces (e.g. web browser to access online email). The consumer does not manage or control the underlying Cloud infrastructure, including network resources, servers, operating system, storage, or even application-layer specific features.
Platform as a Service (PaaS)	In this model, the consumer has the ability to implement applications in the cloud infrastructure through the use of programming languages, libraries, services and tools supported by the cloud service provider. The consumer does not manage or control the underlying Cloud infrastructure, including network resources, servers, operating system, or storage. However, it has control of the implemented applications and, possibly, of the hosting environment configurations related to the same applications. Examples can be Microsoft Azure (Microsoft, 2017), Salesforce (Salesforce, 2017) and the Google App engine (Google, 2017).
Infrastructure as a Service (IaaS)	The consumer has the capacity to provision processing, storage, networking and other key computing resources (usually through virtualized environments). The consumer can implement and run software (e.g., operating system and applications) according to his needs. The consumer does not manage or control the underlying Cloud infrastructure; however, it has control over operating systems, storage, deployed applications, and possibly limited control of certain network security components such as a host firewall.

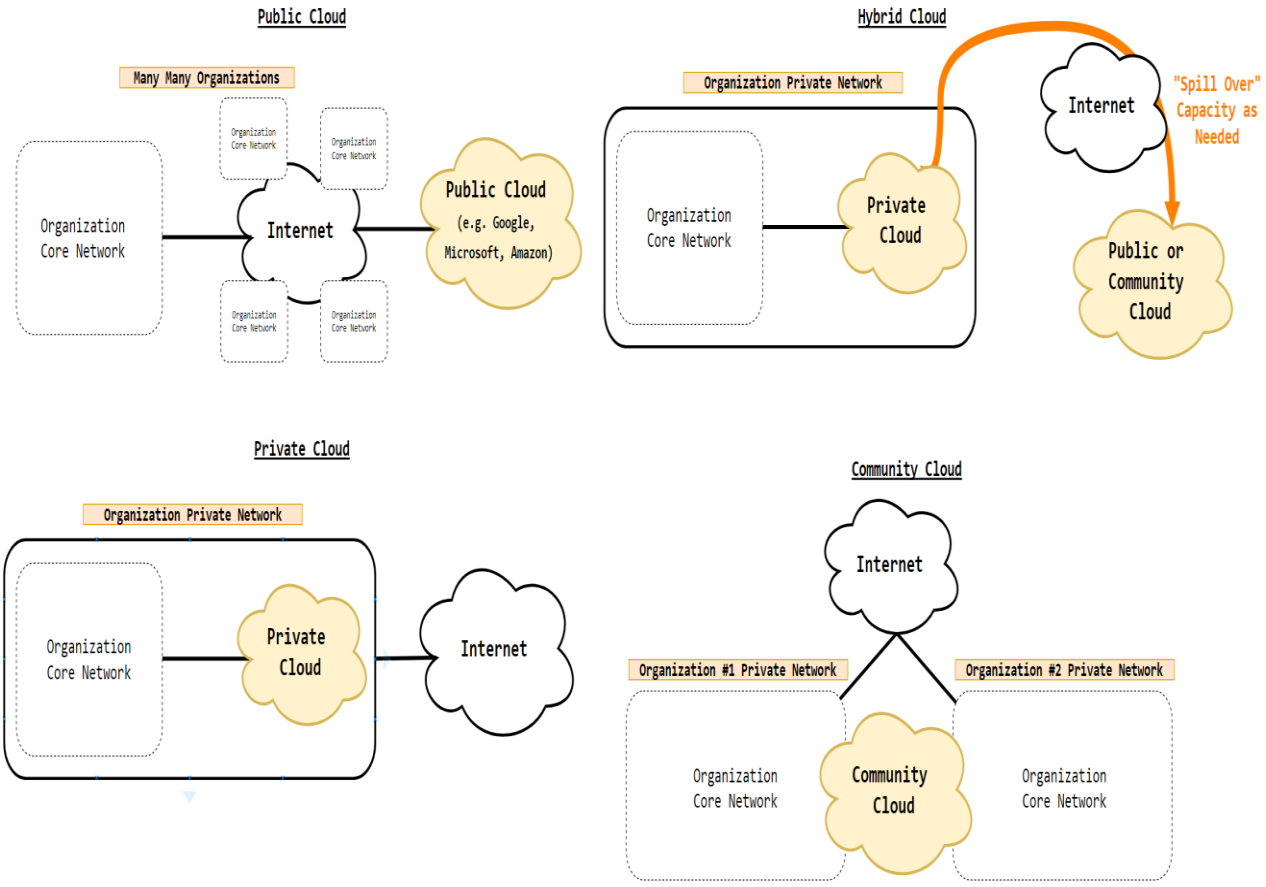
2.1.2 Cloud Deployment Models

Cloud Computing offers four different deployment models. The organizations' choice of model depends on the comparison between its requirements, whether regarding information or business processes, and the model that best meets those requirements. The deployment models and their main characteristics are presented in Table 2, as in Figure 2. (Goyal, 2014; Mell & Grance, 2011)

Table 2 - Cloud Computing Deployment Models. Adapted from (Goyal, 2014; Mell & Grance, 2011)

Cloud Deployment Models	
Model	**Description**
Community Cloud	A Community Cloud infrastructure is provisioned for the exclusive use of a specific consumer's community, composed of organizations that have common goals (mission, security requirements and compliance). Cloud computing infrastructure can be owned, managed and operated by organizations who are part of the community, by a third party or even by a combination of the two. It can exist within the premises of the organization as well as outside it. An example of a Community Cloud may be the use of shared computing infrastructure exclusively by two or more entities within the government (or health sector), which have the same compliance, privacy, and security requirements.
Public Cloud	The Public Cloud infrastructure is provisioned for open use by the general public. The Public Cloud infrastructure can be owned, managed and operated by an organization that sells computer services, by an academic or governmental organization, or by the combination of the various parties. It exists within the premises of the organization that provides the services.
Hybrid Cloud	The Hybrid Cloud infrastructure is made up of two or more distinct cloud infrastructures (public, private or community) which remain unique entities, but are interconnected through technology (proprietary or standardized) that enables the portability of information and applications. (e.g., Relocation of backups between Clouds).
Private Cloud	The Private Cloud infrastructure is provisioned for the exclusive use of a single organization comprising multiple internal consumers (e.g. Business Units). The Private Cloud infrastructure can be owned, managed and operated by the organization itself, by a third party or by the combination of the two. It can exist both inside and outside the organization's premises.

Figure 2 - Cloud Computing Deployment Models integration. Adapted from (Miller et al.,2009)



2.1.3 Cloud Computing Differentiating Features

From an architectural perspective, there is still much confusion surrounding the similarities and differences between the Cloud Computing models and the conventional computing models. It is also unclear how these similarities and differences impact organizational, operational and technological approaches to information and network security practices. Table 3 presents some characteristics that are considered differentiating with respect to the comparison between conventional computing and Cloud Computing, which were taken into account for the elaboration of this dissertation from a security-focused point of view. (Mell & Grance, 2011; CSA, 2011)

Table 3 - Cloud Computing Differentiating Features (Mell & Grance, 2011)

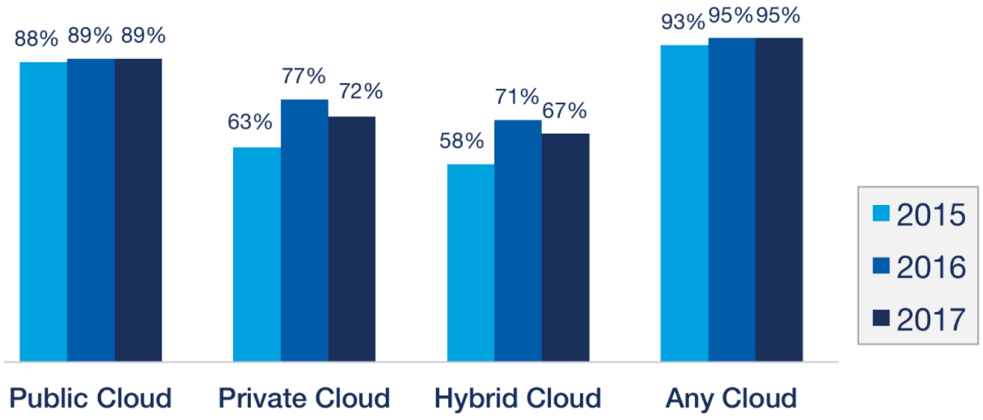
Cloud Computing Differentiating Features	
On-Demand Self-Service	Consumers can unilaterally provision computing resources (e.g., Time the customer wants to use the service or Storage) as needed, automatically and without requiring human interaction with the Cloud Computing service provider.
Broad Network Access	Cloud computing services are available through the network (via the Internet) and are accessed through standardized mechanisms that come from the use of heterogeneous client platforms (e.g. smartphones, tablets, laptops, desktops, among others).
Resource Pooling	The computing capabilities of the Cloud service provider are grouped to serve multiple consumers through a multi-tenant model, with different physical and virtual resources dynamically allocated and reallocated according to the needs of consumers. There is a perception of location independence in the sense that the consumer generally has no control or knowledge about the exact location of the resources provided to him, yet he may have the ability to specify the location at a higher abstraction level (e.g. country, data center). Examples of resources can be storage, processing, memory, and bandwidth.
Rapid Elasticity	Resources can be provisioned quickly and elastically (in many cases automatically) to scale up or scale down quickly and according to the needs of the consumer. For the consumer, the resources available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
Measured Service	Cloud Computing service providers automatically control and optimize resources utilization by leveraging measurement capabilities at an abstraction level appropriate to the type of service provided (e.g. storage, processing, bandwidth, and active user accounts). The use of resources can be monitored, controlled and reported, thus providing transparency of the service used for both the provider and the consumer.

2.1.4 Cloud Computing Adoption

In order to better define the type of target audience for a cloud security readiness assessment model, attempts were made to understand the Cloud models' evolution in terms of adherence. Furthermore, the author tried to be aware of which deployment models are used most to better define which KPI such a model should focus on as part of the assessment (e.g. SLAs in Public Cloud should be more detailed and strict than Private Cloud).

As illustrated by the graph in Figure 3, there has been an evolution in the use of cloud models ("Any Cloud"), which has motivated even more this work. The main reason for such growth is the need for organizations' IT teams to respond to business requirements, both in terms of cost reduction and also with regards to ubiquity, flexibility, efficiency, and immediacy. However, due to these requirements and needs (usually imposed by the organization's senior management), the analysis and evaluation of security-related risks and prior mitigation is often neglected by IT teams when moving information assets to the Cloud. The results presented in the graph are based on a survey which asked 1,002 IT professionals about their adoption of cloud infrastructure and related technologies. Forty-eight percent of the respondents represented enterprises with more than 1,000 employees. The margin of error is 3.07 percent. (Weins, 2017)

Figure 3 - Respondents Adopting Cloud. Extracted from (Weins, 2017)



According to Weins (2017), companies using cloud are leveraging multiple public and private clouds. That is, on average, they are running applications on 1.8 public clouds and experimenting with an additional 1.8 public clouds. They are also running applications on 2.3 private clouds and experimenting with an additional 2.1 private clouds. This may indicate that companies, in general, are experimenting with the option of putting in place a multi-cloud strategy. A multi-cloud strategy is the use of two or more cloud environments to minimize the risk of service availability failure, loss and corruption of data, loss of privacy, vender lock-in or the possibility of malicious insiders in the single cloud. Service unavailability can occur due to the breakdown of hardware, software or system infrastructure. A multi-cloud strategy can also improve overall enterprise performance by avoiding "vendor lock-in" and using different infrastructures to meet the needs of diverse partners and customers. (Pareek, 2013)

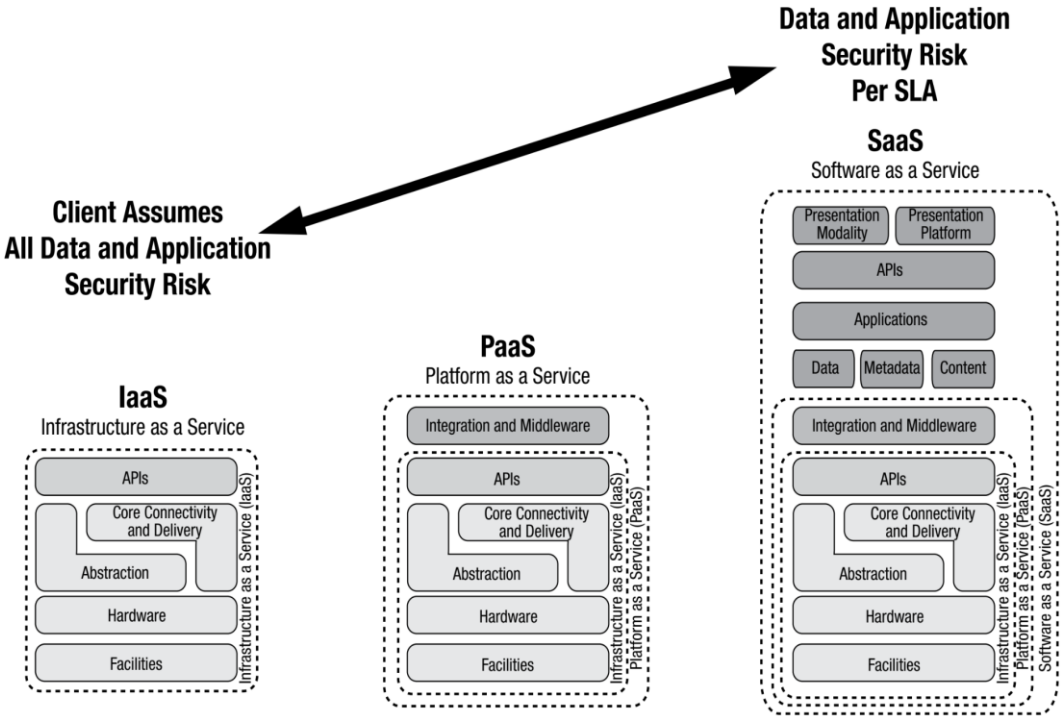
2.2 Cloud Computing and Security

In general, security controls in Cloud Computing are not very different from the security controls in any other IT environment. However, the different cloud computing

service/deployment models and their use can translate into additional risks for an organization.

The overall security level of an organization is characterized by the maturity of the controls implemented to mitigate risk. These controls are implemented in a number of layers, from physical security, network security, human resource security, to information and application security. In cloud computing environments, the consumer's responsibilities across the various security domains and their respective controls vary depending on the service model used. In SaaS environments, the security controls scope is negotiated in the legal contract between the consumer and service provider in terms of service level agreements (SLA), privacy and compliance. In the IaaS offering, the cloud service provider is responsible for ensuring the security of the abstraction layer and the underlying infrastructure, while the remaining components are fully supported and managed by consumers (e.g., Operating system and installed applications). Finally, in the PaaS model the platform security is the service provider's responsibility, however, the consumer is responsible for the security of the applications developed within the platform. These differences are represented in Figure 4.

Figure 4 - Security integration with different service models. Extracted from (ISACA, 2012)



Understanding the impact of these differences between service/deployment models and how they are deployed is a key factor for organizations planning to manage security risk.

2.2.1 Cloud Computing - Possible Security Benefits

The economic, technological and ecological benefits of Cloud Computing have been discussed frequently, but it is worth noting that there are numerous additional potential security benefits related to the use of Cloud Computing resources. The risk assessments and analyses that are carried out by consumers with regards to cloud service providers should be balanced with a review of existing security benefits because for many organizations (e.g. SMB) the use of Cloud Computing might improve their overall security maturity level across the different security areas. Cloud Computing has significant potential to improve the security and resilience of its consumers. Table 4 shows some of the possible security benefits of using Cloud Computing (ENISA, 2009).

Table 4 - Potential Security Benefits of Cloud Computing. Extracted from (ENISA, 2009)

Potential Security Benefits of Cloud Computing	
Benefits of Scale	All types of security measures have a lower cost when implemented on a large scale. That said, the same amount of security investment buys better protection. Some benefits of scale can be: • By default, most cloud service providers have the needed economic resources to replicate content in multiple locations. In this way, they increase the levels of redundancy and fault tolerance, as well as allow the elaboration of Disaster Recovery procedures. • Threat Management - Most cloud service providers have the economic ability to hire security specialists to deal with specific threats, while small and medium-sized enterprises typically only hire professionals with a more IT generic profile. • Better ability to respond to incidents such as cyber-attacks.
Security as a differentiator in the market	When organizations begin a process of analyzing Cloud services, security is one of their primary concerns. Consumers will make their decisions to purchase Cloud services based on the reputation of each provider in terms of confidentiality, integrity, and resilience, as well as the security services that are provided. This is one factor that can motivate Cloud service providers (in general) to improve their security practices.
Rapid, smart scaling of resources	A Cloud service provider has the ability to dynamically relocate resources for filtering, traffic shaping, encryption, among others, to increase support for defense measures (e.g. DDoS attack) when an attack is occurring or is imminent to happen.
Audit and evidence-gathering	Since the IaaS model is usually based on virtualization technology, it supports on-demand cloning of servers. If there are suspected security breaches, the consumer may, for example, remove an image from a machine to perform a forensic analysis in a controlled environment (without downtime).

Chapter 3 Related Work

This chapter presents the work that is somehow related to the topic chosen for this work. The chapter begins with a general presentation of the security risks associated with Cloud Computing and then presents some work in the areas of risk analysis for Cloud Computing and Cloud Readiness and Maturity Level.

3.1 Security Risks in Cloud Computing

This Section reviews known potential Cloud-specific risks. Since the list of potential risks associated with using Cloud Computing resources is very extensive and related to different service and implementation models, it was decided to compile some of the more relevant potential risks for the scope of this document, as we can see below.

Loss of Governance
Governance is the set of processes, technologies, laws, and policies that affect how an organization is managed and controlled. Governance also includes the relationships between the different stakeholders involved in an organization, as well as its objectives. IT governance assumes itself as a subordinate mechanism of overall corporate governance, with the mission of incorporating the intrinsic value of IT into all aspects of the organization. (Mille, 2009).

When using Cloud Computing infrastructures, the consumer has to give control (governance) of different variables to the service provider, which can affect security. At the same time, SLAs may not offer a commitment on the supplier's part regarding security services, i.e. there is a lack of visibility on the consumer's side regarding the technical security measures put into place in the cloud service provider's infrastructure. (CSA, 2011; ENISA, 2009)

Lock-In
As far as we know, and according to the investigation that has been done, there are no procedures or tools that guarantee the portability and interoperability of data, applications, and services. This may make it difficult for a Cloud services consumer to migrate these same services from one provider to another or even to its on-premises infrastructure. This translates into the risk of dependence on a particular provider (CSA, 2011).

Cross-border legal requirements
Cloud computing service providers are often cross-border, and in general, different countries have different legal requirements, especially with respect to private personal information. The cloud service consumer may be violating regulations in other countries

by storing, processing, or transmitting data within the provider's infrastructure, that is, without taking into account the required compliance controls. In addition, government entities in the country where the Cloud infrastructure is located may require access to entity information with or without adequate notification.

It is therefore necessary that, when the Cloud service provider operates outside the consumer's territory, in countries with different legislation, the consumer identifies all legal requirements to ensure that he is not violating the laws of that country by storing and processing his data through the provider's infrastructure (ISACA, 2012).

Isolation Failure

As noted earlier, the Multi-Tenancy feature and the resource sharing through virtualization is one of the key features of Cloud Computing. The failure of isolation mechanisms that separate components such as storage, memory, and network from different consumers (tenants) can translate into a high-level risk. In this multitenant environment, it is essential that the shared resources be totally isolated and protected so that there is no data disclosure by other tenants, for example in situations of resource relocation. In recent years, vulnerabilities of such shared technologies have been used by attackers to launch attacks on cloud infrastructures (Kazim & Zhu, 2015).

Compliance Risks

There are organizations that make considerable investments to achieve certification of compliance with certain standards (industry standards or regulatory requirements). These certifications may be called into question when migrating services to the Cloud, for example:

- If your Cloud Computing service provider is unable to demonstrate evidence that complies with the same standards or
- If the Cloud Computing service provider does not allow consumers to perform cloud audits to verify if the controls implemented are in accordance with their internal policies.

In some cases, the use of Public Cloud Computing services means that certain types of compliance cannot be achieved, such as PCI DSS (ENISA, 2009).

Management Interface Compromise

To manage their infrastructure, consumers of Public Cloud Computing services typically use a management interface accessible through the Internet that allows access to a broad set of resources. This translates into a high risk, especially if the interface is vulnerable to Web attacks (ENISA, 2009).

Data Protection

Cloud Computing can pose several data protection risks to Cloud Computing customers and suppliers. In some cases, it may be difficult for a consumer to effectively check

provider's data manipulation practices and thereby ensure that data is processed in a legal way. This problem is aggravated in cases of multiple information transfers (e.g. between federated clouds) (ENISA, 2009).

Data Disposal

When a Cloud Computing services consumer requests the provider to delete a particular resource, such a request may not result in the complete deletion of the corresponding information. Due to the very nature of the Cloud, where storage is usually shared by multiple consumers, proper data disposal may in some cases be difficult to achieve. In this way, the provider must ensure adequate measures of information destruction after the contracts have been terminated, in order to avoid the recovery and dissemination of critical and sensitive information for the consumer (ISACA, 2012).

Malicious Insider

The damage that can be caused by malicious insiders on the Cloud provider side carries a high level of risk to the consumer. Such a risk stems from the fact that Cloud architectures require certain professionals with access privileges to the underlying systems and their data, such as system administrators (Kazim & Zhu, 2015).

Insecure Data Segregation

It is necessary to understand how the data is segregated by the provider and especially if it uses encryption for the data in transit and/or stored. The cloud provider should also provide evidence that the encryption schemes used were designed and tested by experienced experts as encryption can compromise availability. (Heiser & Nicolett, 2008)

Availability

Briefly, availability is the extent to which the full set of computing resources of an organization is accessible and usable. Availability may be affected temporarily or permanently, and a loss may be partial or complete. Denial of service attacks, equipment outages, and natural disasters are some of the threats to availability. The concern is that most of the downtime is unpredictable and can affect the organization's mission. The availability of Cloud Computing may be affected as follows (Jansen & Timothy, 2015):

- Temporary Failure: Although in general the architectures of Cloud Computing environments are designed to ensure high availability and reliability in the services offered, they may also have certain periods in which service failures or performance damages occur.
- Prolonged and permanent failures: There is a possibility that a cloud provider may have serious problems, such as bankruptcy or loss of premises, which affect the service for long periods or cause complete downtime.
- Denial of Service Attacks.

3.2 Literature Review

The work (Saripalli & Walters, 2010) presents a quantitative risk and impact assessment tool called QUIRC which consists in assessing the security risks associated with six key categories related to security objectives (confidentiality, integrity, availability, multi-trust, auditability and usability) on a Cloud Computing platform. The quantitative definition of risk is proposed as a product of the likelihood of a threat event occurring and its potential impact. The overall platform security risk for a given application belonging to a given security category is the average over the cumulative sum of the threats that map to that category. In addition, it is also necessary to take into account a weight that represents the relative importance of a given category to a particular organization. By using expert-based rankings on the likelihood and consequence of threats, this framework adopts the wideband Delphi method as a scientific means to gather the information needed to assess security risks. Although this framework has advantages, the challenge and the difficulty of applying this approach is the meticulous collection of historical data for the threat events probability of occurrence calculation, which requires data entry from the entities that are being evaluated (Cloud Computing service providers).

The work (Sangroya et al., 2010) presents a risk analysis approach from a Cloud Computing services consumer perspective. This approach consists in analyzing data security risks before the consumer places their sensitive data in the Cloud. The main goals of this work are to help service providers ensure their customers data security as well as help them identify the risks associated with placing critical assets in the Cloud. There is a lack of structured approaches that can be used for risk analysis in Cloud Computing environments and the approach suggested in this paper (based on a trust matrix) is a possible step in analyzing data security risks as well as it appears to be adaptable for automating risk analysis.

Wang et al. (2012) proposes the use of attack-defense trees to perform a threat analysis in the Cloud Computing context. Attack trees are a deductive threat-modeling approach that can be used to explore the several ways in which an attacker can accomplish an attack target. Defense trees can be used to increase an attack tree so that it is possible to explore how protection measures prevent an attacker from having success. Previous work has shown how defense trees can be used to support decision making when considering the most economical protection measures to be used. The main shortcoming of such an approach in Cloud Computing environments relates to obtaining sufficient information and knowledge about the infrastructure of the various stakeholders involved in order to perform the analysis.

The OPTIMIS project, funded by the European Union (among others) carried out an investigation on the Cloud Computing risk assessment, which is largely summarized in one of its results (Jiang et al., 2012). In short, the project has developed a risk

assessment method that can be applied at different stages of the cloud service provisioning lifecycle - both at the time of implementation as well as when the service is in operation. The risk can be assessed from the service provider's or infrastructure provider's perspective (service providers offer economically efficient services with assessed and guaranteed environmental impact using hardware resources provided by infrastructure providers). Several functional components and a high-level architecture have been identified to support risk assessment from both parties perspective. The results of the risk assessment are used in the broader scope of the framework developed for the OPTIMIS Cloud, for example, in the context of access control (allowing the implementation of new services). One aspect of the OPTIMIS risk assessment method addresses the problems associated with the uncertainty of evaluating different infrastructure providers (during implementation or migration) caused by the lack of information provided by them. An essential part of this aspect is an approach called Dempster-Shafer Analytical Hierarchy Process (DsAHP), a technique that aims at supporting decision making using incomplete information on a number of criteria (e.g. compliance with industry standards).

Recognizing the specific challenges to implement Cloud Computing risk assessment, the concept of Risk Assessment as a Service (RAaaS), where continuous and on-demand risk assessment can be carried out, has been proposed (Kaliski Jr & Pauley, 2010). Some Cloud Computing properties are presented, aligned with the essential characteristics of NIST (Mell & Grance, 2011), which make the process of risk assessment a great challenge and, thus, motivate the need for RAaaS.

In the work (Loebbecke et al., 2011), a model to evaluate an organization's Cloud Readiness is presented. This model uses a practical method called "magic matrices" to evaluate which services, applications and business processes are prepared to be adapted to the Cloud Computing concept. When using this method, the organization begins by comparing different service and deployment models considering various criteria such as data privacy or even cost-effectiveness. Next, the magic matrices method is applied, which, in a first phase, consists of identifying which services can be migrated to Cloud. Then, evaluation criteria (magic matrices) are defined and for each service to be evaluated its level is checked against the pre-defined criteria (e.g. bandwidth level gets better or not?). Finally, there is a categorization phase, which consists in assigning to each evaluated service a level of Cloud Readiness (e.g., Cloud Ready, not yet Cloud ready, unlikely to be assessed as cloud-ready in the next few years).

3.3 Review of Standards

The European Network and Information Security Agency (ENISA) has released a cloud computing risk assessment report highlighting the security advantages and risks related to consuming Cloud Computing services. Through the same report, it provided some

viable recommendations and designed a set of criteria to assess the risk of adopting Cloud services. (Catteddu & Hogben, 2009).

CSA (2011) presents a set of best security practices, putting together guidance ranging from 14 different domains involved in governing or operating the cloud (e.g. Cloud Architecture, Governance and Enterprise Risk Management, Compliance, and Audit). This effort provides a practical, actionable roadmap to consumers wanting to adopt the cloud paradigm safely and securely. The guidance serves as a high-level primer for chief executives, consumers, and implementers wishing to adopt cloud services as an alternative or supplement to traditional infrastructure.

The international standard ISO/IEC 27017:2015 provides guidelines supporting the implementation of information security controls for both cloud service customers and cloud service providers (ISO/IEC, 2015). These guidelines for information security controls applicable to the provision and use of cloud services provide not only additional implementation guidance (having cloud security in mind) for relevant controls specified in ISO/IEC 27002 (ISO/IEC, 2013), but also additional controls with implementation guidance that specifically relate to cloud services. Proper use of the controls provided by this standard relies on the organization's information security risk assessment and treatment.

The ISACA (2012) document provides practical guidance regarding the decision process surrounding the adoption of cloud services. First, a short theoretical description of cloud concepts is presented before identifying the most common risk areas and threats in the cloud landscape. Also, an approach to cope with these cloud-specific risk areas and threats is provided, enabling effective analysis and measurement of risk using items such as decision trees and checklists outlining the security factors to be considered when evaluating the cloud as a potential solution. This guide is meant for all current and potential cloud users who need to ensure protection of information assets.

The work presented in (ODCA, 2017) addresses the maturity of an IT organization's business and technology capabilities in specific domains and across cloud service models, such as Software as a Service (SaaS); Platform as a Service (PaaS); Infrastructure as a Service (IaaS) and others. Although is not used specifically for security, it has a well-defined process for maturity assessment and some valuable insights were taken for the present dissertation.

Throughout this state-of-art investigation, the author verified that there is a gap regarding the existence of maturity models that enable an organization to assess its maturity level specifically from a Cloud security perspective, as well as to identify the specific controls (e.g. security policies and processes, prevention mechanisms, contracts) that mitigate risk arising from the use of Cloud Computing services.

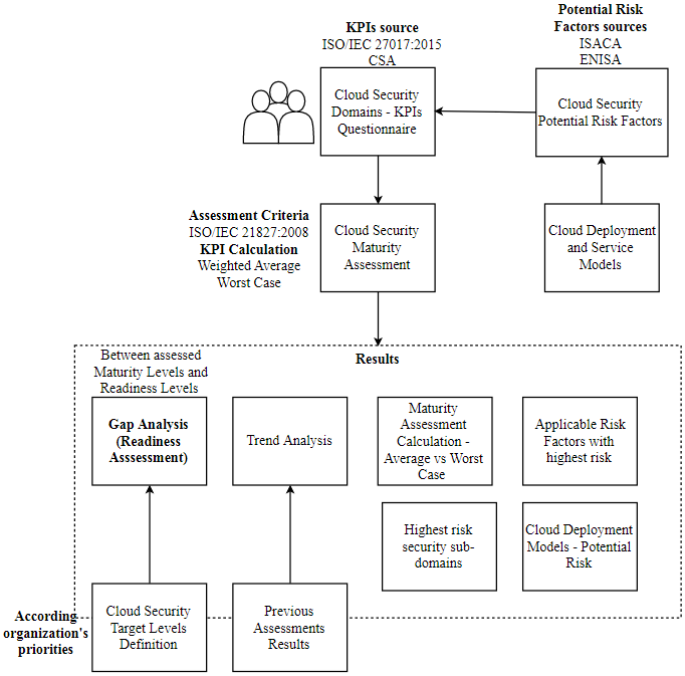
Chapter 4 A solution to assess the *readiness* and potential risk on Cloud environments

Regarding the scope of this work, initially, the intention was to conceive more effective methods to deal with the limitations identified in the related work, as well as to adapt and improve their findings. Based on the analysis of the related work, a solution was created that is more aligned with the business management and decision-making of an organization's senior management regarding Cloud services that are being used or services that could be migrated to Cloud Computing. To this end, ideas from Cloud Readiness previously proposed in the literature were adapted to the information security reality. Concepts and guidance from well-known standards, e.g. ISO/IEC 27017:2015 (ISO/IEC, 2015) were also considered during our work. This chapter presents the conceptualized Cloud Security maturity assessment model and the corresponding developed tool that translate the model's theory into practice.

4.1 Model description

A high-level representation of the designed model and its different components' integration is exhibited in Figure 5. The model provides an approach that, through input providing assessment of security Key Performance Indicators (KPI), materialized in a questionnaire, enables an organization to evaluate the extent to which it is sufficiently prepared to use cloud computing services, taking into account the diverse range of security areas and its potential risks.

Figure 5 - Assessment model overview - Components integration



After completing the maturity assessment, it will be possible for an organization to define, in a more grounded way, which areas should be considered as priorities for future investments. These future investments should not only increase cloud security maturity, but also reduce the risk of using Cloud Computing services.

In addition, the model incorporates risk concepts which can help an organization improve their security risk management processes. The author believes that, by establishing a relationship between the degree of maturity for a particular security domain and the potential cloud-specific risk factors, it is possible for an organization to assess the main potential risk factors it faces when using certain Cloud Computing services. Each potential risk factor is described as well as mapped to cloud deployment models and service models, in terms of applicability.

It is important to highlight that, as Cloud service customers are adopting a multi-cloud strategy (according Section 2.1.4), the designed model tries, as closely as possible, to be directly related to the customer's security needs in a generic way and not focused on the specific functionalities provided by different CSPs (although CSP security controls assessment is also part of it). Based on that, the customers themselves are able to compare different providers and select them based on the specific need (e.g. For SaaS would choose one specific provider and for PaaS another one).

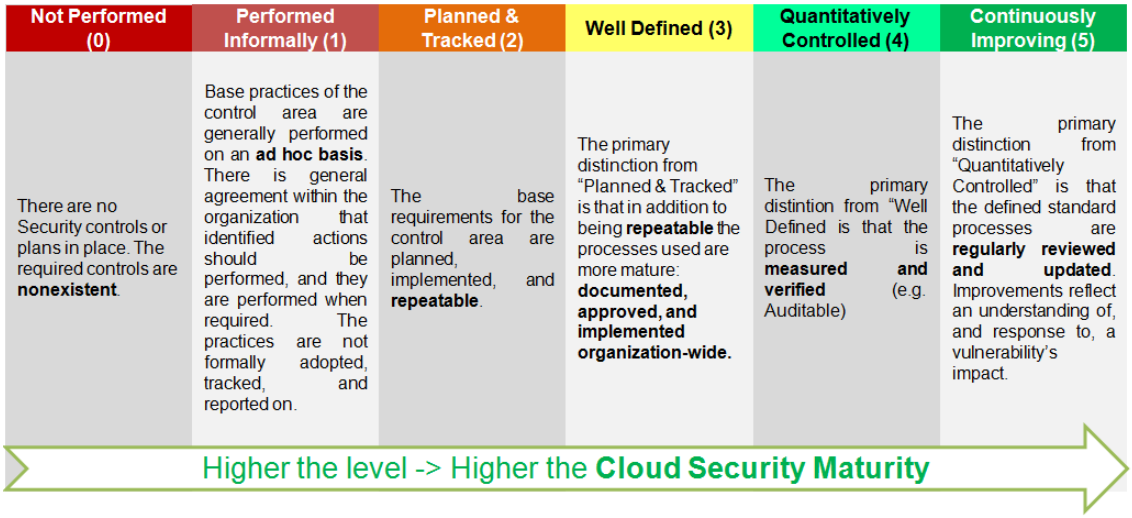
4.1.1 Readiness Assessment

Regarding the core object of this work, the Cloud Security Maturity Assessment, it was necessary to design a model to evaluate whether specific controls (e.g. processes, technology, employee awareness, etc) are in place on the organization that is being assessed and, if so, to which extent they are aligned with the organizations target readiness level. As such, a maturity approach was implemented. Maturity approaches come from the field of quality management (Fraser et al., 2002) and were extended to the IT field in order to manage software development (Team, S. U., 2011). As time went by, those approaches were applied to organizations' processes. Maturity is described as the state of being complete, perfect or ready ("readiness"). As a result, in order to be "ready", an organization needs to follow an evolutionary path to reach the desired target state, starting from initial state (Lahrmann et al., 2011). Maturity models provide that path since they are composed of multiple maturity levels of a domain and can be used to assess an organization's maturity level or for organizational development (Lahrmann et al., 2011). The inherent advantages when using this approach comes from the best practices and evolutionary paths they offer and from the fact that they can be used to assess the actual state of an organization and/or to define what and how organizations can improve their processes and capabilities in a specific field.

For the purpose of this work, this maturity approach has been adapted to the Cloud Security field. With regards to the model's measurement scale that, for each Key

Performance Indicator (KPI), enables the current Cloud security maturity level evaluation, the evaluation criteria of a known and stable standard was adapted, in this case, the ISO/IEC 21827:2008 (ISO/IEC, 2008). This standard describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering and aims to facilitate an increase in the maturity of the security engineering processes within an organization. The result of the criteria adaptation to the Cloud security domain is presented in Figure 6.

Figure 6 - Cloud Security maturity level evaluation criteria. Adapted from ISO/IEC 21827:2008



For each Cloud security domain (containing one or more KPIs) that is being assessed, the model considers two types of calculation of its maturity level, the weighted average (according to the score for each of the domain KPIs) and the worst case, which represents the lower maturity level among the KPIs. In the beginning of the project only the average maturity level for each security domain was used, but during the model designing process it became clear that with this kind of approach, by the end of the assessment, there would be the risk of losing track of important KPIs with low maturity levels for some specific security domains. By having the worst case representation of the security domain maturity level it is possible to identify domains which, although having an average maturity level that does not require the organization's attention after the assessment, have one or more KPIs with a low maturity level which should be improved according to the organization's priorities.

For the maturity assessment to cover the most relevant cloud security areas, the solution assessment KPI had to be carefully chosen. The KPI are basically questions relating to certain cloud security domains that must be answered in order for the "interviewer" to be able to draw conclusions regarding the maturity level of those domains and compare to the organization's target levels. Based on that, for KPI definition, the solution has as the primary source the ISO/IEC 27017:2015 (ISO/IEC, 2015). It was chosen as primary source because it was developed by the recognized International Organization for

Standardization (ISO) and most organizations are already trying to improve their overall security maturity by being compliant with other ISO standards such as the ISO/IEC 27002:2013 (ISO/IEC, 2013), that is the ISO/IEC 27017:2015 foundation (ISO/IEC, 2015). Therefore, by using this solution, an organization can identify areas that must be improved to achieve ISO/IEC 27017:2015 compliance and the author believes this could be a way to motivate organizations using it. An important remark regarding this decision is that, although the guidance provided in ISO/IEC 27017:2015, the solution also has some generic security insights from ISO/IEC 27002:2013. For the scope of this work only the Cloud-specific guidance was used as input for the KPI definition. With this approach, it is assumed that an organization has (or should have) controls already in place to be compliant with the ISO/IEC 27002:2013.

Following an in-depth analysis of other references, it was decided that the CSA guidelines (CSA, 2011) would complement the ISO/IEC 27017:2015 in the way that it covers additional relevant areas (e.g. Interoperability, Portability) and has a more practical way of exposing its contents, making it easier to understand. With this in mind, mapping between the ISO/IEC 27017:2015 domains and the CSA domains was performed in an attempt to find domains to complement the already existing KPIs to have the best of both worlds, resulting in a first KPI list providing better coverage regarding relevant cloud security.

4.1.2 Potential risk identification

As was mentioned above, the model also has some risk concepts incorporated within it. With this, the objective was not only to create some awareness of the possible risk factors associated with the use of cloud services, but also to help organizations with their risk management processes by identifying cloud-specific risks that should be calculated depending on each organizations reality and risk appetite.

The model provides an identification of the most relevant risk factors related to the use of Cloud Computing environments. For risk identification, we have used the (ENISA, 2009) and (ISACA, 2012) references. The decision to use these references was based on the fact that, following an in-depth investigation of several different sources of information (whether scientific or not), it has become clear that most of the relevant cloud risk factors were present in those two references. Furthermore, because the (ISACA, 2012) reference includes a mapping between the cloud risk factors and the different cloud service and deployment models, this has also been included in the model in an attempt to make the organization aware of the potential risks associated with a specific cloud service/deployment model that is being used or is being analyzed for future adoption. For example, an organization might want to outsource some internal services to a public cloud (deployment model) and chose the IaaS (service model) to do it. By using the designed assessment model, the organization would be able to identify very easily the potential risk factors affecting the chosen service/deployment models

and to take some action to mitigate it. In addition, the model establishes a relationship between the cloud security readiness assessment KPIs and the potential risk factors. This is accomplished through the mapping between KPIs and its potential risk factors. With this approach an organization can be aware of the risks it may run if specific KPIs do not have an acceptable cloud security maturity level and it can then define a roadmap to mitigate such risks.

For the organization to assess the possible impact on its cloud services assets in the event that a threat occurs, the model also includes impact criteria as well as a mapping between the risks and their possible impact. Table 5 contains a description of each impact event that is being used in the model. The impact criteria were based on (ISACA, 2012).

Table 5 - Impact criteria for potential risk factors. Extracted from (ISACA, 2012)

Impact Criteria	
Impact Event	**Description**
Unavailability	The asset is unavailable and cannot be used or accessed by the organization. The cause can be accidental (failure of the CSP infrastructure), intentional (distributed Denial-of-Service [DDoS] attacks or legal (subpoena of the database holding all data in a case of multitenancy architecture where one client's data are subject to legal investigation).
Loss	The asset is lost or destroyed. The cause can be accidental (natural disaster, wrong manipulation, etc.) or intentional (deliberate destruction of data).
Theft	The asset has been intentionally stolen and is now in possession of another individual/enterprise. Theft is a deliberate action that can involve data loss.
Disclosure	The asset has been released to unauthorized staff/enterprises or to the public. Disclosure can be accidental or deliberate. This also includes the undesired, but legal, access to data due to different regulations across international borders.

4.2 Tool description

The developed prototype tool features map the aforementioned model components for cloud security maturity assessment and potential cloud-specific risk factors assessment. The prototype was developed in Microsoft Excel as this software is widely used by organization's senior managers and made it possible to translate the theoretical design model into practice in a non-complex way. The tool layout can be found in more detail in Annex C.

4.2.1 Readiness Assessment

For each KPI maturity level calculation, the tool provides a combo box that enables the selection of the correspondent maturity level (e.g. Performed Informally) according questionnaire feedback. According the evaluation criteria defined in Figure 6, the prototype not only presents the average and worst case result, but also gives a visual representation of the results, as can be seen in Figure 7.

Figure 7 - Tool KPI Maturity Level calculation (average and worst case) example

DOMAINS	SUBDOMAINS	SECTION	KEY PERFORMANCE INDICATOR (KPI)	MATURITY LEVEL	
				Avg	Worst Case
Information Security Policies		1	Total Score for domain ->	Quantitatively Controlled	Performed Informally
Management direction for information security	Policies for information security	1.1.1	Does your institution have an information security policy considering the Cloud topic (policy and procedures in accordance with its use of cloud services) that has been approved by management?	Performed Informally	
			Has it been published and communicated to all relevant parties?	Continuously Improving	
	Review of the policies for information security	1.1.2	Does your institution review the Cloud policy at defined (and regular) intervals to encompass significant change and monitor for compliance?	Continuously Improving	

Keeping in consideration that the organizations being assessed by the tool might want to understand what the reference is for each KPI, there are also two columns, as shown in Figure 9, that indicate the KPI reference sections if a more in-depth explanation is needed or if the organization wants to be in compliance with a specific reference like ISO/IEC 27017:2015. Summing up, in total, 14 relevant cloud security domains and 94 KPI across those domains have been adopted for the tool, as shown in Figure 8.

Having an extensive list of KPIs could possibly run the risk of having the "interviewed/interviewees" losing attention during the assessment, so attempts were made to find possible intersections between the different KPIs defined and, consequently, to remove them. For example, if two KPIs were similar within the same

security domain, only one of them would remain in the tool. As such, the number of KPIs has been reduced without losing relevant cloud security coverage for the maturity assessment. Figure 7 shows examples of KPIs that belong to the tool in the domain "Management direction for Information Security".

Figure 8 - Tool domains for Cloud Security Readiness assessment

DOMAINS	SECTION
Information Security Policies	1
Organization of Information Security	2
Human Resource Security	3
Asset Management	4
Access Control	5
Cryptography	6
Physical and Environmental Security	7
Operations Security	8
Communications Security	9
System acquisition, development and maintenance	10
Supplier Relationships	11
Information security incident management	12
Compliance	13
Interoperability and Portability	14

By looking at Figure 7 or Figure 10, it is possible to observe that some KPIs might be bold. The reason for that is to identify the KPIs which have a maturity level that depends on the maturity level of other KPIs. Taking the Figure 7 KPIs as an example (in the Information Security Policies domain), if the maturity level for the KPI "*Does your institution have an information security policy considering the Cloud topic that has been approved by management?*" is "*Not performed*", then for the KPI "*Has it been published and communicated to all relevant parties?"* the maturity level will inherently be the same as it depends on the above KPI (if it has an "*information security policy considering the Cloud topic"* or not). The KPIs that depend on other KPI maturity levels are indented below them.

The tool has an open text field "Rational" (presented in Figure 9) that should be used by the "interviewer" to insert, for each KPI, the current maturity level evidence provided by the "interviewed". Those pieces of evidence can be technological controls which have been implemented such as a firewall or even process IDs that identify the organizations' internal processes. The rationale might then be used at a later time, if needed, for example, to provide evidence of compliance in a future assessment.

The developed prototype can also be used to compare results of different assessments over time, making it possible to monitor the evolution of the maturity level for each KPI and for each security domain.

Figure 9 - Tool maturity assessment layout example

MATURITY LEVEL		TREND ANALYSIS		Rational (e.g. Existing controls, process ID, applicable risks, etc)	POTENTIAL RISK FACTORS	ISO27017:2015 REFERENCE	CSA REFERENCE
Avg	Worst Case	Previous Assessment (avg)	Trend				
Quantitatively Controlled	Performed Informally	Well Defined	⇧				
Performed Informally		Performed Informally	⇨		R3, R15, R18	5.1.1	NA
Continuously Improving		Quantitatively Controlled	⇧				
Continuously Improving		Quantitatively Controlled	⇧		R1, R3, R18, R27, R38	5.1.2	
Well Defined	Planned	Planned	⇧				
Well Defined		Quantitatively Controlled	⇩		R3, R9, R10, R38	6.1.1	
Quantitatively Controlled		Performed Informally	⇧				

The analysts using the tool can examine the past performance (e.g. maturity levels from previous years) of an organization, along with current maturity levels, to determine how the organization should perform in the future (by defining target maturity levels). The previous assessment results are based on average results and should be inserted manually in the column "Trend Analysis -> Previous Assessment (avg)". Then, based on the current assessment results, the tool provides a visual representation to facilitate the identification of KPIs or security domains which improved, remained the same or got worst (according to Figure 10).

Figure 10 - Tool trend analysis results

DOMAINS	SUBDOMAINS	SECTION	KEY PERFORMANCE INDICATOR (KPI)	MATURITY LEVEL		TREND ANALYSIS	
				Avg	Worst Case	Previous Assessment (avg)	Trend
Asset Management		4	Total Score for domain ->	Continuously Improving	Planned	Quantitatively Controlled	⇧
Responsibility for assets	Inventory of assets	4.1.1	Does the CSC has an inventory of assets accounting for information and assets stored in the cloud computing environment?	Continuously Improving		Quantitatively Controlled	⇧
			Does the CSC inventory has records indicating where the assets are maintained?	Continuously Improving		Quantitatively Controlled	⇧
	Removal of cloud service customer assets	4.1.2	To which extent does the CSP provide a documented description regarding the termination of service process covering return and removal of CSC's assets followed by the deletion of all copies of those assets from the CSP's systems?	Continuously Improving		Quantitatively Controlled	⇧
			To which extent does the description contains a list of all the assets and the sched	Continuously Improving		Quantitatively Controlled	⇧
Information classification	Labelling of information	4.1.3	Does the CSC labels information and associated assets maintained in the cloud computing environment in accordance with the information classification scheme adopted by the organization?	Planned		Quantitatively Controlled	⇩
				Continuously Improving		Quantitatively Controlled	⇧

Finally, in the readiness assessment, it is also possible to verify the potential risk factors IDs related with each security sub-domain. The author believes that these risks might

have a higher risk level (if applicable) in case the maturity level for that sub-domain is low.

4.2.2 Potential Risk identification

To accomplish the model's potential risk factors identification, the tool provides a table that identifies the risk factors related to the use of Cloud Computing environments, as well as a detailed description of it in another column. In total, the tool incorporates 41 cloud-specific risk factors.

Figure 11 - Tool Potential Risks Identification layout example

RISK ID	CLOUD SERVICE MODELS			CLOUD-SPECIFIC RISK FACTORS	DESCRIPTION
	IaaS	*PaaS*	*SaaS*		
R1	X	X	X	Legal transborder requirements	CSPs are often transborder, and different countries have different legal requirements, especially concerning personal private information. The enterprise might be committing a violation of regulations in other countries when storing, processing or transmitting data within the CSP's infrastructure without the necessary compliance controls. Furthermore, government entities in the hosting country may require access to the enterprise's information with or without proper notification.
					Customer data may be held in multiple jurisdictions, some of which may be high risk. If data centres are located in high-risk countries (e.g., those. lacking the rule of law and having an unpredictable legal framework and enforcement, autocratic police states, states that do not respect international agreements, etc), the corresponding sites where the data resides could be raided by local authorities and data or systems subject to enforced disclosure or seizure. Note that we are not implying here that all subpoena law-enforcement measures are unacceptable, merely that some may be so and that some legitimate seizures of hardware (which appear to be rare) may affect more customers than the targets of

Taking into account the aforementioned (Section 4.1) relation between the cloud security readiness assessment KPIs and its potential risks, a risk ID has been assigned for each risk. With this approach, the relationship works as follows: for each existing security sub-domain in the readiness assessment, we have included a column that holds the potential applicable risk factors IDs (as shown in Figure 9).

Furthermore, to establish a relationship between the cloud risk factors and the different cloud service and deployment models, the tool includes one column per Cloud service and deployment model and the applicability mapping is done through the use of an "X". Figure 11 gives an example of one risk and two descriptions, ENISA and ISACA descriptions, respectively, and their mapping to the different Cloud Service Models (the "X" means that the risk is applicable to that specific model).

Finally, as illustrated in Figure 12, we have also included a column with the potential risk source references and another one to map between the impact events from the pre-defined impact criteria (Table 5) and the potential risk factors.

Figure 12 - Tool Potential Risks impact mapping

DESCRIPTION	CLOUD DEPLOYMENT MODELS				SOURCE	IMPACT CRITERIA AFFECTED
	Hybrid Cloud	*Private Cloud*	*Public Cloud*	*Communitary Cloud*		
CSPs are often transborder, and different countries have different legal requirements, especially concerning personal private information. The enterprise might be committing a violation of regulations in other countries when storing, processing or transmitting data within the CSP's infrastructure without the necessary compliance controls. Furthermore, government entities in the hosting country may require access to the enterprise's information with or without proper notification.					ISACA	
Customer data may be held in multiple jurisdictions, some of which may be high risk. If data centres are located in high-risk countries (e.g., those. lacking the rule of law and having an unpredictable legal framework and enforcement, autocratic police states, states that do not respect international agreements, etc), the corresponding sites where the data resides could be raided by local authorities and data or systems subject to enforced disclosure or seizure. Note that we are not implying here that all subpoena law-enforcement measures are unacceptable, merely that some may be so and that some legitimate seizures of hardware (which appear to be rare) may affect more customers than the targets of	X		X	X	ENISA	Disclosure

4.2.3 Resulting Dashboards

After the assessment is concluded, the results are presented in two different dashboards that the tool provides. One of the dashboards being the "Executive Dashboard" which demonstrates high-level information about the gap between the maturity level achieved and the target levels (readiness state), as well as a trend analysis and the comparison between the average maturity level and the worst case.

The other dashboard, the "Technical Dashboard" is more technical, and more related to the potential risk factors which come from the established relationship (or mapping) between the questionnaire sub-domains and the potential risk factors IDs mentioned on Section 4.1.2. The following sub-sections explain the two dashboards, the Executive Dashboard and the Technical Dashboard, (and correspondent charts) in more detail.

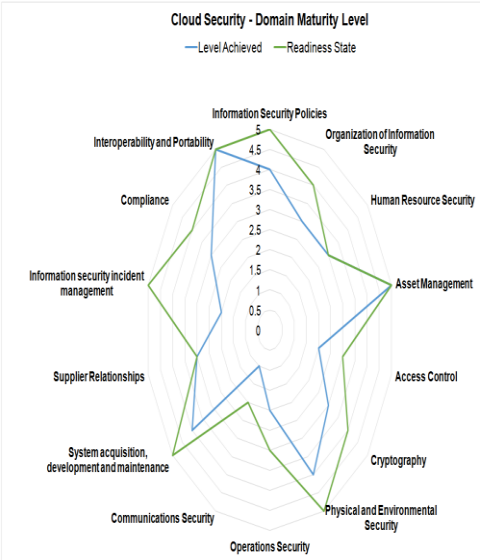
Executive Dashboard

Cloud Security Domain Maturity Level

This tool component is probably the most important that the tool provides, in the way it allows the organization to define the Target Readiness State (according to its priorities) and, consequently, to perform the gap analysis between the maturity level achieved after the assessment and the Target Readiness State ("Readiness assessment"). The visual representation provided allows the organization to identify the areas which have to be improved in the future. Furthermore, it can be a good way for IT Security managers or CISOs to justify investments to their organization's board. Figure 13 presents a simulated example of this gap analysis chart. By analyzing the example it is possible to identify that the information security incident management domain is far away from the desired readiness levels and, in turn, define it as being one of the highest priority security domains in terms of future improvement investments.

Figure 13 - Cloud Security Domain Maturity Gap Analysis

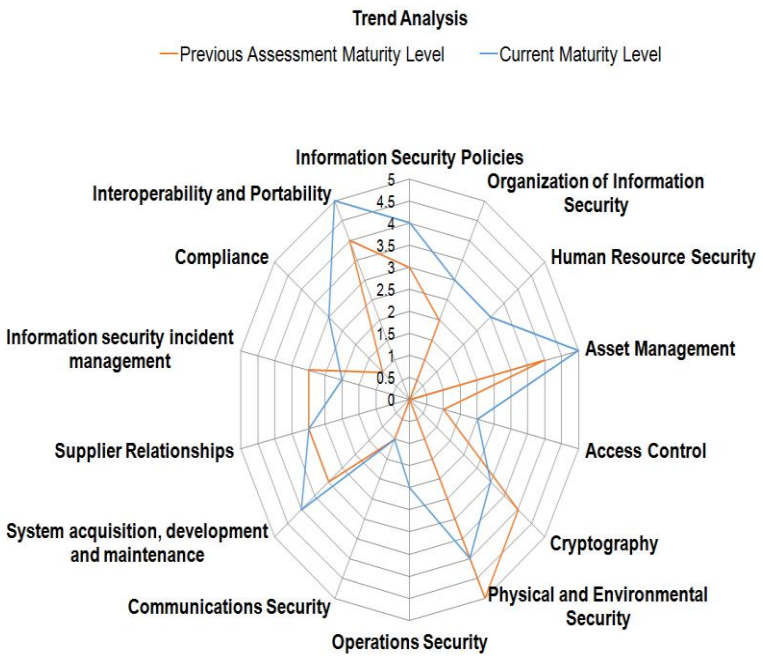
Security Domain	Target Readiness State
Information Security Policies	Continuously Improving
Organization of Information Security	Quantitatively Controlled
Human Resource Security	Well Defined
Asset Management	Continuously Improving
Access Control	Well Defined
Cryptography	Quantitatively Controlled
Physical and Environmental Security	Continuously Improving
Operations Security	Well Defined
Communications Security	Planned
System acquisition, development and maintenance	Continuously Improving
Supplier Relationships	Well Defined
Information security incident management	Continuously Improving
Compliance	Quantitatively Controlled
Interoperability and Portability	Continuously Improving



Trend Analysis

The Trend Analysis chart, of which an example is displayed in Figure 14, should be used to compare results of different assessments over time, making it possible to monitor the evolution of the maturity level for each security domain. Analysts using the tool are able to examine the past performance (e.g. maturity levels from previous years) of an organization, along with current maturity levels, to determine how the organization should perform in the future (by defining target maturity levels) and to gain some insight regarding the evolution between assessments as well (e.g. why some security domain decrease their maturity level).

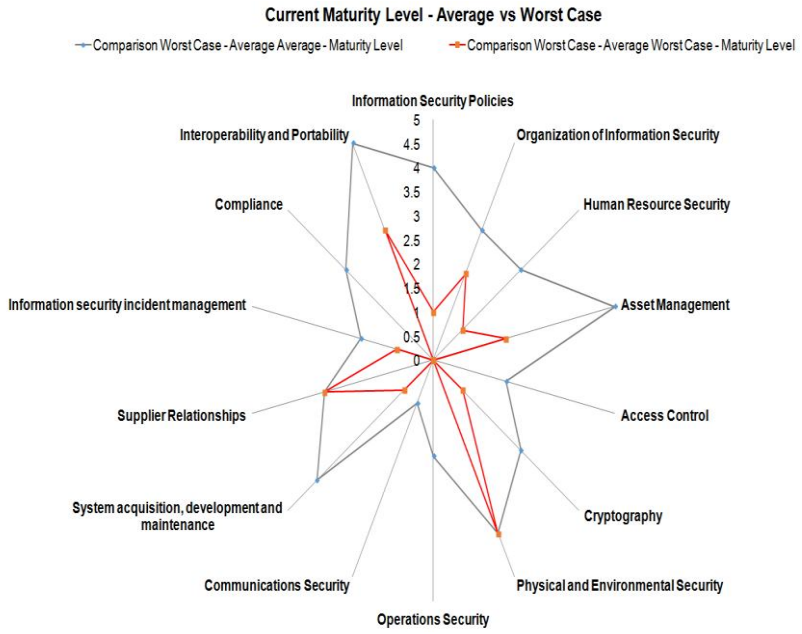
Figure 14 - Cloud Security Trend Gap Analysis



Average vs. Worst Case

As has already been mentioned in Section 4.1, for each security domain that is being assessed, the tool performs two types of calculation for its maturity level, the average, and the worst case. This chart basically gives a visual representation of the differences between these two types of calculation, for each domain. With it, it is possible to identify the domains which, although having an average maturity level that does not require the organization's attention after assessment, they have one or more KPIs that have a low maturity level and should be improved according to the organization's priorities. Figure 15 exhibits an example that demonstrates the Compliance domain has one KPI that has a maturity level of 0 ("Not Performed"). For large organizations that have compliance as one of its most critical domains, this worst case identification could be an important contribution.

Figure 15 - Cloud Security maturity comparison between average and worst case



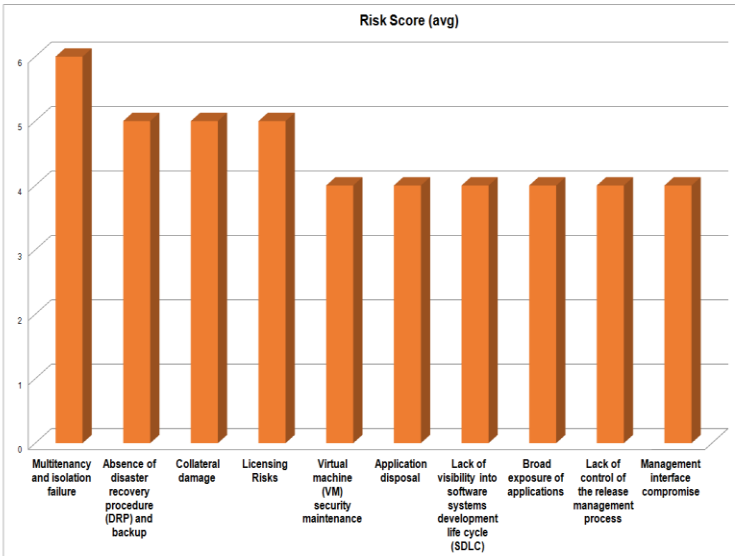
Technical Dashboard

Top 10 Potential Risk Factors

Through the established relationship between the security sub-domains (and its assessment maturity level) and the potential risk factors that were explained in Section 4.1.2, the prototype provides a chart that contains the top 10 potential risk factors (as can be seen in Figure 16). The authors believe that this information could prove useful for an organization from a risk management perspective. Nevertheless, this information only represents an estimate of the potential risk factors based on the maturity level achieved, so each organization being assessed should calculate the risk level based on its environment, using specific risk calculation formulas.

Figure 16 - Cloud Security Top 10 Potential Risk Factors

Potential Risk Level	
Value	**Description**
1 and 2	Marginal
3	Minor
4	Moderate
5	Significant
6	Major

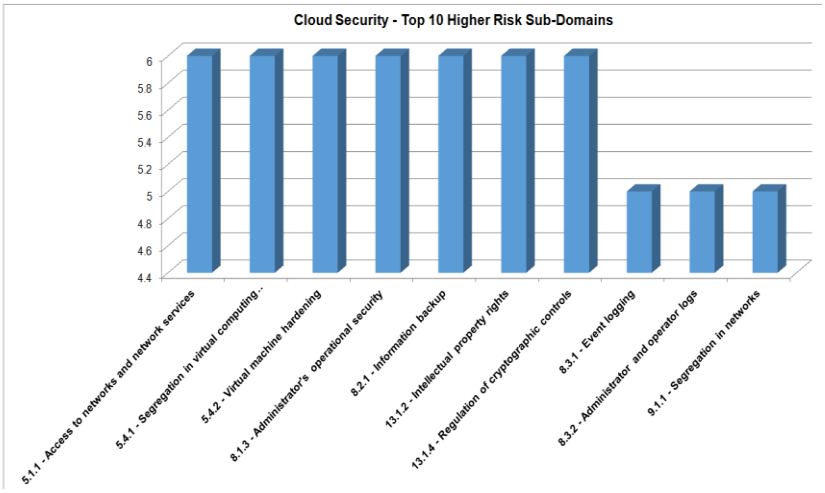


Top 10 Higher Risk Sub-Domains

As for the "*Top 10 Potential Risk Factors*", this chart also comes from the established relationship between the security sub-domains and the potential risk factors. The author believes that by identifying (through a chart) the sub-domains with a higher risk, an organization will be able to easily identify the sub-domains whose maturity level requires improvement. Figure 17 represents an example of the chart provided by the developed prototype.

Figure 17 - Cloud Security Top 10 Higher Risk Sub-Domains

Potential Risk Level	
Value	**Description**
1 and 2	Marginal
3	Minor
4	Moderate
5	Significant
6	Major

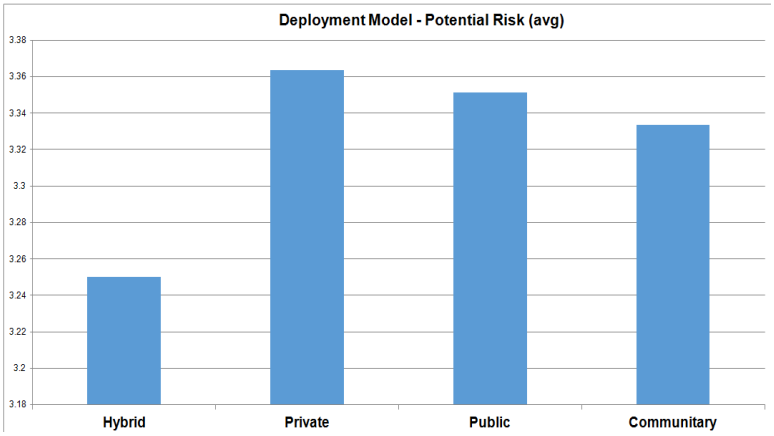


Cloud Deployment Models - Potential Risk

The chart Cloud Security Potential Risk for Cloud Deployment Models (exhibited in Figure 18) was built using the same methods as the other Technical Dashboard charts. For organizations analyzing what deployment model best fits its interests, this chart can be helpful to compare the different models from a security maturity approach perspective.

Figure 18 - Cloud Security Potential Risk for Cloud Deployment Models

Potential Risk Level	
Value	**Description**
1 and 2	Marginal
3	Minor
4	Moderate
5	Significant
6	Major



4.3 Process for Assessment

To effectively assess an organization and determine a roadmap of actions and planning, the authors believe that a predictable process is needed so that organizations using the tool can follow it effectively. The Cloud Security Maturity Assessment process that should be followed is presented in more detail in Table 6 (as well as in Figure 19).

Figure 19 - Cloud Security Maturity Assessment Process

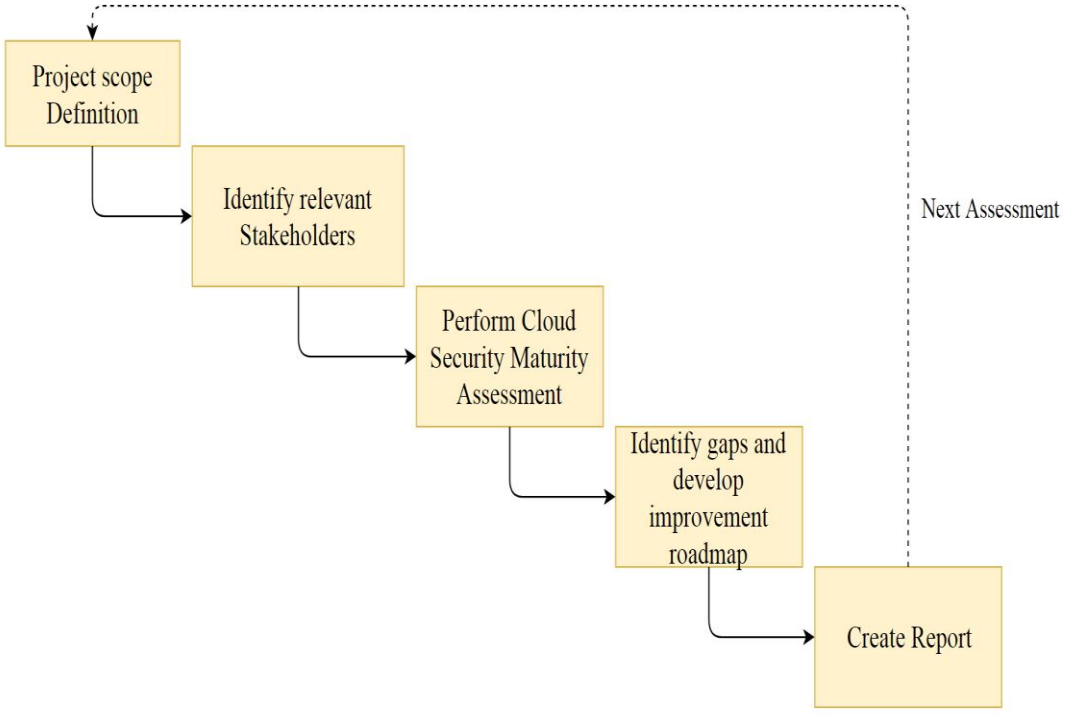


Table 6 - Cloud Security Maturity Assessment Process description

Cloud Security Maturity - Process for Assessment	
Phase 1 Project Scope Definition	The scope of the project should be defined. Above all, it is important to identify the specific Use Case that the organization wants to analyze. For example, an organization might have already assets in the Cloud and want to analyze what controls should be put in place if they want to get more mature in terms of Cloud Security. Also, target readiness levels should be defined in this phase. Examples of Use Cases might be: Cloud Computing Services adoption (e.g. only SaaS), Maturity level improvement for existing CSCs, etc.
Phase 2 Identify Relevant Stakeholders	This team should be comprised of a multidisciplinary group of individuals, from senior management to a more technical level. Stakeholders are likely to come from the ranks of security, IT governance, compliance, legal, senior management. Also, CSPs could be included here if an organization is using the tool to compare them.
Phase 3 Perform Cloud Security Maturity Assessment	By using the tool, conduct the interviews based on the KPIs. Section 4 helps in how to use the tool. For the interviews, the right personnel have to be chosen for each domain. For example, if one is assessing the information security incident management domain then the interviewed has to be someone that is familiar with all the processes and technology associated with the domain.
Phase 4 Identify Gaps and develop improvement roadmap	After using the assessment tool, potential gaps between the results obtained and the target readiness levels must be identified (defined by the organization that is being assessed). The tool helps in identifying the gaps (Section 4.3). Then, define the roadmap with the organization regarding the areas and correspondent security controls that should be considered for future improvements and to achieve the target readiness states. Investment needed might be included in the roadmap.
Phase 5 Generate Report	Develop a report that includes the assessment findings as well as the roadmap for future improvement and the justification for the decisions that were taken.

Chapter 5 Tool Evaluation

In this chapter validation of the developed solution's applicability is presented. This Section has as objective to demonstrate that the tool that was created adds value to organizations in general and that the results obtained with the evaluation are consistent with what the author idealized. Section 5.1 explains the method and criteria used to evaluate the developed tool. The evaluation participants are presented in Section 5.2. Finally, Section 5.3 discusses the results.

5.1 Method of evaluation

Although initially the idea behind the evaluation was to perform a Proof of Concept by doing an exhaustive assessment to a specific organization, the scope of the evaluation was changed due to some constraint related with the author's availability and the organization's confidentiality as well. Based on that, it was decided that the evaluation should be leveraged on tool demonstrations to information security experts that have relevant roles on the large companies they are working for. Through this method of evaluation the author is able to assess if the tool has applicability to real world scenarios, from an utility perspective. These experts and companies they work for were selected based on the following criteria:

- The information security experts had to have a decision-making role (with regards to information/IT security) inside the company they are working for. One of the primary work objectives since the beginning was to design a model (and implement a correspondent tool) to support organizations' decision-making, so the expert's feedback might indicate if we achieved it.
- The information security experts had to have solid knowledge in Cloud Computing security and compliance topics.
- The information security experts had to have 5 or more security-related years of work experience.
- Each one of the security experts works for a different company;
- The companies they are working for has interest in evaluating a tool like the one developed.
- Each company has to belong to a different area of activity, with preference for the banking and critical infrastructures area, as well as information security advisory area (probably are the ones using the tool to assess its customers).
- Each company should have an employed manpower of over 1000 employees. This criteria is important for the evaluation because the larger the company, the more likely it is to have a high Security maturity level.

The tool onsite demonstration was done to three different information security experts (Section 5.2) in different individual meetings. The demonstration consisted in the following steps:

1. **Contextualize** – In this stage the author contextualized the information security experts with regards to the dissertation objectives and motivation (Section 1).

2. **Process for Assessment** – After contextualizing, the authors have explained the steps that make up the process for assessment in order for the participants to understand what would be done if their companies were to be assessed with the developed tool.

3. **Tool Demonstration** – The demonstration of the prototype tool consisted in going through the different solution features in a detailed way, by simulating a small assessment and presenting the results. In the readiness assessment menu, as there were too many KPIs to cover all in the meetings, the author tried to focus on the domains that the information security expert was more interested.

4. **Questions** – Although during the tool demonstration the participants were making questions and providing feedback regarding what could be improved, the author reserved a space in the final of the interview for specific questions that the expert might still have.

5. **Questionnaire** – After concluding each assessment demonstration, the author delivered a questionnaire (Annex A and Annex B) to the participant in order to assess his/her level of satisfaction with regards to the tool and also to understand if we have achieved the previously defined objectives. The results and correspondent analysis can be found in Section 5.3.

5.2 Participants

This Section presents the information security experts that have evaluated the created tool. The participants chosen have a profile that corresponds to the pre-defined criteria (Section 5.1) and are the following:

- EY Portugal – Cyber Security Advisory Senior Manager

The first participant is a Senior Manager from EY (former Ernest and Young) Portugal. EY is one of the four largest professional services companies in the world (the big four), present in 150 countries, in 728 offices, and with more than 190,000 employees. It provides assurance (including financial audit), tax, consulting and advisory services to companies.

By having a member of a company that provides cyber security advisory services and has a large experience in doing security assessments, the author was able to verify through the evaluation if the created tool would be used by them to perform cloud security maturity assessments and to which degree it would be beneficial to their customers that consume Cloud Computing services or are analyzing that possibility.

- EDP – SOC Manager

One of the chosen participants is a SOC Manager at EDP (Energias de Portugal) group, which is a company from the energy sector with a consolidated position in the Iberian Peninsula, both in the production, distribution and commercialization of electricity and gas. The EDP Group has a strong world-wide presence in the energy sector, being present in Portugal, Spain, France, the United States, United Kingdom, etc. Worldwide, it counts with more than 10 million customers and more of 12,000 employees. As in the past EDP performed a security assessment before and during migrating services to the Cloud, the author believed that by having their feedback regarding the created prototype tool, it would be possible to evaluate to which extent it would have been useful for them the use of the tool during the migration phase. Also, has they have already a satisfactory Cloud security maturity level, what their recommending improvements are.

- Caixa Económica Montepio Geral – IT Security Manager.

Caixa Económica Montepio Geral belongs to Associação Mutualista Montepio and is responsible for the group's banking activities. Its business focuses on retail intermediation by attracting resources from small and medium-sized customers and granting loans to individuals, micro-enterprises, SMEs, individual entrepreneurs and social economy institutions. As this company belongs to the banking sector, and usually banking institutions have strong security and compliance requirements, and are constantly being audited by third-parties, the authors believe that the feedback from their expert helps to assess the applicability to these strict security environments.

5.3 Analysis of Results

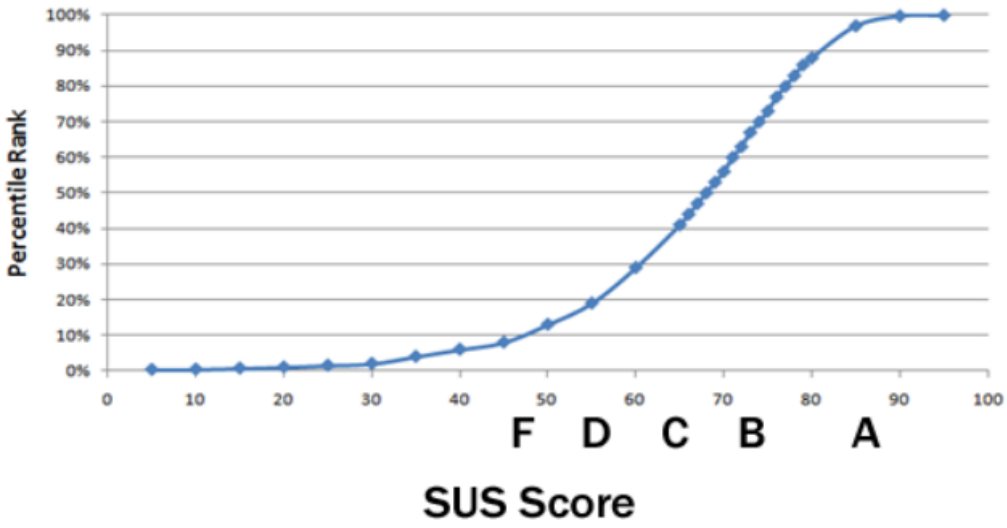
As explained on the evaluation method (Section 5.1), after looking at the prototype demonstration, the participants answered two questionnaires designed to measure the tool's utility and usability level. The questionnaires were developed considering the method presented by (Brooke, 1996). In this Section the results that came from those questionnaires (Annex A and Annex B) filled by the participants are presented. These results are then discussed taking into account the author's perspective and expectations. Participants responded to these utility and usability questionnaires using a scale from 1 to 5, with 1 meaning "totally disagree" and 5 meaning "I totally agree". The questions might have a positive character, where we expected the participants to answer the value 5 (or close to it), or a negative character, where we expected participants to answer the

value 1 (or close to it). In order to obtain the questionnaire result for each participant, the answer value for each positive character question is subtracted with value 1. With regards to the negative character questions its value is subtracted to 5. In this way each question is valued from 0 to 4 and the sum of all responses reflects the questionnaire result questionnaire in a value between 0 and 40 (for the utility questionnaire as it is made up of 10 questions) or between 0 and 20 (for the usability questionnaire as it is made up of 5 questions). To convert this value to a percentile, that is, a value between 0 and 100, the utility result value is multiplied by 2.5 and the usability result is multiplied by 5. This evaluation method was based on (Brooke, 1996) that is focused on measuring usability with a system usability scale (SUS), and adapted to the utility area.

5.3.1 Utility

Participants answered a questionnaire designed to measure the tool's utility level. The objective with this utility questionnaire was to assess if the participants would use the tool for their company's environment and if they consider it as an important contribution regarding the study field of Cloud security maturity and potential risk assessment. The questionnaire can be found in Annex A and the final results regarding the tool's utility are shown in Table 7. The utility questionnaire was based on a set of ten questions, so the SUS results range from 0 to 40. Final results are shown in Table 7.

Figure 20 - SUS usability scoring curve. Extracted from (Sauro, 2011)



The mean value of the percentiles obtained is approximately 76.6, which on the SUS scale corresponds to a "B". As can be seen in Figure 19, it corresponds to the second highest grade in the scale so we can conclude that in general the participant's feedback was positive.

Table 7 - Results obtained from the utility questionnaire - SUS

Utility results		
User	**SUS Result**	**Percentile (%)**
U1	29	72.5
U2	35	87.5
U3	28	70
Average Percentile (%)		
76.66		

There are several main positive aspects regarding the results of this utility questionnaire:

- The participants considered that the tool represents an important contribution to the security maturity level (readiness) evaluation of an organization regarding cloud computing. The participants believe that, if an organization has a clear picture of what are the readiness levels they want to achieve, the tool, by enabling the gap analysis between current maturity levels and those readiness levels, will facilitate the roadmap definition that will make it possible to reach that readiness achievement. This was the major goal with this work. Still on this matter, the participants also considered as an important contribution the fact that the tool allows assessing the maturity level for each different cloud security domain because an organization might want to only perform the assessment to particular domains considered as more priority according its business and compliance requirements.

- The "Trend Analysis" feature that enables the comparison of the current Cloud security maturity level with previous assessments was considered very useful by the participants in the way it, for example, enables the easy identification of areas or specific KPI that are not evolving (in terms of maturity) as planned by the organization.

- Regarding risk concepts, the participants found the tool interesting in the way it facilitates the evaluation of the possible risk factors associated with the adoption of Cloud Computing services and, consequently, their organization's cyclical risk management internal processes.

- The participants considered as an important contribution the fact that the tool supports decision-making regarding critical points related to Cloud Computing services. The participants agreed that, by having a clear picture of the gap between the maturity level an organization has and the readiness level it should have, the senior management can take grounded decisions for the future (e.g. invest in specific security areas to improve the cloud security maturity level).

- Even though the answer was not consensual for all the participants, they considered as useful the fact that the tool helps in estimating variations of possible (Cloud-related) risk due to changes in the IT structure of an organization, regarding Cloud Computing services adoption. An example of this feature could be: imagining that an organization wants to use a specific service (e.g. email) through Cloud SaaS, through the use of the tool the organization would be able to identify very easily the potential risks that apply to the SaaS deployment model. This is accomplished through the mapping between the cloud deployment models and the potential risk factors.

- Finally, the participants considered that the tool helps organizations to define what it's needed for them to be aligned with globally-recognized best practices for Cloud Security (e.g. achieving compliance with ISO/IEC27017:2015). This was one of the author's major concerns when choosing the right references for the tool KPI definition, therefore, the evaluation validated that goal.

Although the answers from the different participants were not always consensual, the following aspects were considered by the author as having a less positive result:

- The participants believe that it would not be easy for this tool to be adapted to analyze another IT-Related domain (not Cloud Computing). The reason for including the corresponding question was because the author believes that from a layout point of view the tool could be adapted to other domains. The extensive required effort to adapt would be mostly related to the KPIs definition.

- Although one of the participants believes this tool is an important contribution to the cloud security maturity benchmarking definition per different organization's business unit or activity areas (e.g. banking, utilities, insurance, wholesale), the others did not agree on that. As the benchmarking definition for this Cloud security maturity does not exist (as far as the author was capable to check), the author's perspective is that the tool can help in continuously creating this benchmarking as assessments are being done.

5.3.2 Usability

Comparing to utility, the usability evaluation had less priority for the author, due to the fact that this tool is innovative from a concept perspective and evaluating the utility at this stage tends to be more important. Nevertheless, participants also answered a short questionnaire designed to measure the tool's usability level. The objective with this usability questionnaire was to assess if the participants would find it easy to understand how the different tool features integrate as well as the key features and functionality. The questionnaire can be found in Annex B and the final results regarding the tool's

utility are shown in Table 8. The utility questionnaire was based on a set of five questions, so the SUS results range from 0 to 20.

The mean value of the percentiles obtained is approximately 81.6, which on the SUS scale corresponds to an "A". As can be seen in Figure 19, it corresponds to the highest note in the scale so we can conclude that in general the participant's feedback was very positive.

Table 8 - Results obtained from the usability questionnaire - SUS

Usability results		
User	**SUS Result**	**Percentile (%)**
U1	17	85
U2	18	90
U3	14	70
Average Percentile (%)		
81.666		

There are several main positive aspects regarding this utility questionnaire. The participants considered that most people will learn how to use the tool very quickly has it is easy to locate key features and functionality that the tool provides, being it the readiness assessment or the potential risk factors. Also, that the several options of the tool are well integrated, mostly in the relationship between the security sub-domains maturity and the applicable potential risk factors. Finally the participants could see themselves using the tool on a regular basis to perform assessment from time to time.

Finally, although the answer was not consensual, generically speaking the participants considered that the tool would be more useful if it were web-based, especially for access segregation reasons. Access Segregation through a method like RBAC (Ferraiolo et al., 1995) would allow for example to create access accounts with permissions for specific features like viewing "Executive Dashboards", as well as other accounts for tool administration (e.g. for new KPI insertion). Also it would enable the creation of accounts for auditors that for some reason want to evaluate the maturity level and collect justification evidences. The Trend Analysis feature would also gain functionality with a web-based version of the tool, as the results could be stored in a database and a more complete historical representation of the maturity level evolution through the assessments could be shown.

Chapter 6 Conclusion and Future Work

This chapter presents the work conclusions and draws some future developments that might improve the designed model.

6.1 Conclusions

This work proposes a holistic approach to assess the cloud security maturity within an organization, enabling the gap analyzes between their current cloud security state and satisfactory maturity levels across different security domains. This approach, in turn, helps organizations to define investment priorities in order to achieve satisfactory maturity levels across different security domains. The author believes that when an organization's IT security and business strategies align to meet a satisfactory cloud security maturity level, the organization will be able to achieve a better governance model as well as a more secure and interoperable cloud environment that delivers expected benefits. Consecutively, this will enable the organization to have expected business value that cloud services represent (e.g. immediacy, capability and efficiency gains, flexibility increases) without neglecting important security-related areas.

From the premise that providing a way to assess the Cloud Security maturity level can contribute to improve an organization's management system for information security, the proposed methodology focused on assessing, through the use of created KPIs across different security domains, to which extent an organization meets its cloud security readiness goals. To help organizations in their risk management processes, the created prototype also incorporates potential risk factors that may arise with the use of the different Cloud Computing service/deployment models.

Employing the assessment methodology, the author has not only performed an evaluation which demonstrates the applicability of the proposed and developed prototype, but also gained insights from the evaluation that make them believe the developed work establishes a basis for what is becoming increasingly fundamental in the area of managing cloud security. The author considers that this developed basis is subject to improvements in the future.

6.2 Future work

The developed work assumes that an organization, taking into account its business, security and compliance requirements, is able to define target readiness maturity levels that will serve as input to perform the gap analysis between the current and target maturity states. Nonetheless, that is not always the case for many organizations that

don’t have enough security expertise. Based on that, a possible feature that would improve the developed prototype is the incorporation of cloud security benchmarking concepts across the different areas of activity (e.g. banking, utilities, insurance, etc.). Having that feature, managers performing an assessment would have the ability to define target readiness maturity levels (across the different security domains) through the selection of the area of activity that is most suitable for that specific assessment (based on the organization’s profile). Although it might not be easy to accomplish that improvement, as historical assessment results are needed to define the cloud security benchmarking across different industries, the authors believes that the developed prototype tool can help in continuously creating this benchmarking as assessments are being done.

The author considers that through the developed work, and in order to help organizations decision-making, it’s possible to compare different cloud service providers in the way they influence an organization’s cloud security maturity levels. That can be accomplished by performing different assessments for each provider and comparing the organization’s results. Nevertheless, that process is manual and could be improved through an automatic comparison between the different providers and its services, also taking into account the security risk associated with the choice of each one.

Finally, and based on the evaluation participants’ feedback, a web version of the developed prototype could become beneficial with regards to the implementation of specific features. An example could be the implementation of access segregation through a method like RBAC (Ferraiolo et al., 1995). That would allow creating access accounts with different permission sets depending on the user that is interacting with the tool. For example it would be possible to create an account for board members to allow them to follow maturity levels evolution through the “Executive Dashboards” without having access to other features. Also it would possibly enable the creation of accounts with specific permissions for auditors that for some reason want to verify the organization’s maturity level and collect justification evidences that support those results.

Glossary

CISO

Chief Information Security Officer is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

CSC

Cloud Service Customer is an entity that uses cloud services provided by a Cloud Service Provider.

CSP

Cloud Service Provider is an entity whose business is to provide Cloud services to its customers.

DDos

Distributed Denial of Service is a computer attack where the attacker attempts to make a machine or network resource unavailable to its users through temporary or indefinite interruption of the services that are running on a machine connected to the Internet.

Disaster Recovery

The Disaster Recovery topic involves a set of policies and procedures to enable the recovery of critical infrastructure and systems in the wake of a natural or man-made disaster.

Downtime

The time during which the normal production of a process or system is interrupted, derived from different aspects like computer attack or maintenance procedure.

Finding

A conclusion reached after an investigation.

Insider

Insider concerns to a person who is in a position of power or has access to confidential information in a legitimate manner.

IT

Information Technology

KPI

A Key Performance Indicator (KPI) is a measurable value that demonstrates how effectively a company is achieving key business objectives. Organizations use KPIs to evaluate their success at reaching targets.

Lock-In

Lock-in refers to the restricted or proprietary use of a technology, solution or service developed by a supplier. Regarding Cloud Computing, this technique can be demoralizing because consumers are effectively prevented from switching to alternative providers in a simple and low-impact way.

Multi-Tenancy

A multi-tenant Cloud is a Cloud Computing architecture that allows consumers (customers) to share Cloud Computing resources, whether public or private. The data of each tenant is isolated and should remain invisible to other tenants.

NIST

National Institute of Standards and Technology is an agency that acts in the technological area and that develops measures and sets standards as required by the industry or North American government programs.

On-Premises

The word on-premises is used to identify land or buildings that are owned by a company or organization.

RBAC

Role-based access control is an approach to restricting system access to authorized users. It is a policy neutral access control mechanism defined around roles and privileges. The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to perform user assignments.

SLA

Service Level Agreement is an agreement that set the expectations of consumers with respect to the quality, performance, responsibility and security of the services provided by the CSP.

SMB

Small and Medium Business - are businesses whose personnel numbers fall below certain limits. The criteria for defining the size of a business differ from country to country, with many countries having programs of business rate reduction and financial subsidy for SMEs.

Stakeholders

Stakeholders is a term used in several areas such as project management, media, and software architecture that refers to the interested parties who must be in accordance with the corporate governance practices performed by the company.

Traffic Shaping

Traffic shaping is a term used to define the practice of prioritizing data traffic through the conditioning of network throughput in order to optimize the use of available bandwidth.

References

Brooke, J. (1996). “SUS-A quick and dirty usability scale”. Usability evaluation in industry, 189(194), 4-7.

Catteddu, D., Hogben, G. (2009). “Cloud computing information assurance framework.”. European Network and Information Security Agency (ENISA). Retrieved on 18, November, 2016: https://www.enisa.europa.eu/publications/cloud-computing-information-assurance-framework

CSA (2011). Security guidance for critical areas of focus in cloud computing v3. 0. Cloud Security Alliance. Retrieved on 10, October, 2016: https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf

ENISA (2009). Cloud Computing: Benefits, risks and recommendations for information security. European Network and Information Security Agency. Retrieved on 21, November, 2016: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport

Ferraiolo, D., Cugini, J., & Kuhn, D. R. (1995, December). Role-based access control (RBAC): Features and motivations. In Proceedings of 11th annual computer security application conference (pp. 241-48).

Fraser, P., Moultrie, J., & Gregory, M. (2002). The use of maturity models/grids as a tool in assessing product development capability. In Engineering Management Conference, 2002. IEMC'02. 2002 IEEE International (Vol. 1, pp. 244-249). IEEE.

Google (2017). Google App Engine. Retrieved on 07, September, 2017: https://cloud.google.com/appengine/docs/

Goyal, S. (2014). Public vs private vs hybrid vs community-cloud computing: A critical review. International Journal of Computer Network and Information Security, 6(3), 20.

Heiser, J., & Nicolett, M. (2008). Assessing the security risks of cloud computing. Gartner Report. Retrieved on 07, October, 2016: https://www.gartner.com/doc/685308/assessing-security-risks-cloud-computing

ISACA (2012). Security Considerations for Cloud Computing. Information System Audit and Control Association. Retrieved on 02, November, 2016:

http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/security-considerations-for-cloud-computing.aspx

ISO/IEC (2008). ISO/IEC 21827:2008. Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model, International Organization for Standardization and International Electrotechnical Commission

ISO/IEC (2013). ISO/IEC 27002:2013. Information technology - Security techniques - Code of practice for information security controls, International Organization for Standardization and International Electrotechnical Commission

ISO/IEC (2015). ISO/IEC 27017:2015. Information technology-Security techniques-Code of practice for information security controls based on ISO/IEC 27002 for cloud services, International Organization for Standardization and International Electrotechnical Commission

Jansen, W., & Timothy, G. (2015). Guidelines on Security and Privacy in Public Cloud Computing–Publication 800-144. National Institute of Standards and Technology. Retrieved on 22, November, 2016: https://www.nist.gov/publications/guidelines-security-and-privacy-public-cloud-computing

Jiang, Ming, et al., (2012). "D6. 1.3. 2 Scientific Report on Risk Assessment in OPTIMIS." OPTIMIS project deliverable. Retrieved on 02, November, 2016: http://www.optimis-project.eu/sites/default/files/content-files/document/optimis-public-delievarable-d6132-scientific-report-risk-assessment.pdf

Kaliski Jr, B. S., & Pauley, W. (2010, June). Toward Risk Assessment as a Service in Cloud Environments. Proc. of the 2nd USENIX Conference on Hot Topics in Cloud Computing, 7 Pages.

Kazim, M., & Zhu, S. Y. (2015). A survey on top security threats in cloud computing. Int J Adv Comput Sci Appl (IJACSA), 6(3), 109-113.

Lahrmann, G., Marx, F., Winter, R., & Wortmann, F. (2011, January). Business intelligence maturity: Development and evaluation of a theoretical model. In System Sciences (HICSS), 2011 44th Hawaii International Conference on (pp. 1-10). IEEE.

Loebbecke, C., Thomas, B., & Ullrich, T. (2011, September). Assessing cloud readiness: Introducing the magic matrices method used by Continental AG. In IFIP International Working Conference on Governance and Sustainability in Information Systems-Managing the Transfer and Diffusion of IT (pp. 270-281). Springer Berlin Heidelberg.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology. Retrieved on 02, November, 2016: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Microsoft (2017). What is Azure. Retrieved on 7, September, 2017: https://azure.microsoft.com/en-us/overview/what-is-azure/

Miller, J., Candler, L., & Wald, H. (2009). Information Security Governance-Government Considerations for the Cloud Computing Environment. *Booz Allen Hamilton.*

ODCA (2017). Cloud Maturity Model Rev. 3.0. Open Data Center Alliance. Retrieved on 24, June, 2017: https://opendatacenteralliance.org/article/cloud-maturity-model-rev-3-0/

Pareek, P. (2013). Cloud Computing Security from Single to MultiClouds using Secret Sharing Algorithm. International Journal of Advanced Research in Computer Engineering & Technology, 2(12), 3261-3264.

Salesforce (2017). What is Salesforce? Retrieved on 7, September, 2017: https://www.salesforce.com/products/what-is-salesforce/

Sangroya, A., Kumar, S., Dhok, J., & Varma, V. (2010, March). Towards analyzing data security risks in cloud computing environments. In International Conference on Information Systems, Technology and Management (pp. 255-265). Springer Berlin Heidelberg.

Saripalli, P., & Walters, B. (2010, July). Quirc: A quantitative impact and risk assessment framework for cloud security. In 2010 IEEE 3rd International Conference on Cloud Computing (pp. 280-288). IEEE.

Sauro, J. (2011). Measuring usability with the system usability scale (SUS). Retrieved on 15, August, 2017: https://measuringu.com/sus/

Team, S. U. (2011). Standard CMMI Appraisal Method for Process Improvement (SCAMPI) A, Version 1.3: Method Definition Document.

Wang, P., Lin, W. H., Kuo, P. T., Lin, H. T., & Wang, T. C. (2012). Threat risk analysis for cloud security based on Attack-Defense Trees. In Computing Technology and Information Management (ICCM), 2012 8th International Conference on (Vol. 1, pp. 106-111). IEEE.

Weins, K. (2017). Cloud computing trends: 2017 state of the cloud survey. Right Scale. Retrieved on 7, September, 2017: https://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2017-state-cloud-survey

Appendix A – Utility questionnaire

#	Question	U1	U2	U3
1	This tool represents an important contribution to the security maturity level (readiness) evaluation of an organization regarding cloud computing	5	5	4
2	It is very useful the fact that this tool enables the comparison of the current Cloud security maturity level with previous assessments (and, consequently, the continuous maturity level progress)	5	4	3
3	This tool represents an important contribution to the evaluation of the possible risk factors associated with the adoption of Cloud Computing services	5	5	4
4	One important contribution of this tool is to allow assessing the maturity level for each different (relevant) security domain	4	4	4
5	This tool represents an important contribution to the decision-making regarding critical points related to Cloud Computing services	4	5	4
6	I believe this tool is an important contribution to the cloud security maturity benchmarking definition	3	5	3
7	This tool will help organizations to be aligned with globally-recognized best practices for Cloud Security (e.g. achieving compliance with ISO27017:2015)	4	5	5
8	It will hardly be possible for this tool to be adapted to analyze another IT-Related domain (not Cloud Computing)	4	3	2
9	This tool is useful to estimate variations of possible (Cloud-related) risk due to changes in the IT structure of an organization (e.g. Cloud Computing services adoption)	3	5	3
10	This tool does not facilitate the cyclical execution of the risk management process	2	2	2
	SUS Score	29	35	28
	Percentile	72.5	87.5	70

Appendix B – Usability questionnaire

#	Question	U1	U2	U3
1	It is easy to locate key features and functionality that the tool provides	4	4	4
2	The several options of this tool are well integrated	5	5	4
3	Most people will learn how to use this tool quickly	5	5	4
4	The tool would be more useful if it were web-based	3	5	3
5	The tool is too complicated to use on a regular basis	1	2	2
	SUS Score	17	18	14
	Percentile	85	90	70

Appendix C – Developed Tool Prototype Layout

Ciências ULisboa

Cloud Security Readiness and Potential Risk assessment tool

Introduction

In a world increasingly dependent on the information exchanged through digital media (called the "Information Era"), the evolution of the paradigm of traditional IT solutions for the emerging theme (and more and more convincing) of Cloud Computing is visible. This is due not only to the differentiating characteristics of this type of structure (e.g. *on-demand self-service*, ubiquity, rapid elasticity, flexibility, among others) and to the greater effectiveness in the management and use of IT resources, but also, from a business point of view, the inherent commercial benefits such as cost containment (both capital and operational costs), which fit perfectly into the constantly changing business needs of organizations.

Although the advantages are easily identified from a business point of view, many potential consumers are reluctant to use Cloud Computing services to host their information assets due to the fact that, in the first stage, they deal with the "unknown" (Because they are formatted for the traditional environment), as well as due to the risks and security threats inherent to these environments (in part because of the high degree of exposure of the Cloud services to the Internet). In this context, the Cloud Computing model has particularities that distinguish it from the traditional computing models insofar as the risks are different for each service model in the "Cloud" (IaaS, PaaS, SaaS) as well as for each implementation model (Private, Public, Community, Hybrid).

The goal of this framework is, among others, to help potential consumers evaluate their potential security risk factors regarding the adoption of cloud computing services, as well as to verify their degree of maturity at this level (readiness) in a qualitative way, supporting decision-making regarding the implementation of appropriate risk management and mitigation mechanisms.

This maturity assessment is based on questionnaire and covers 14 different security domains each with its KPIs to be evaluated.

Process for Assessment

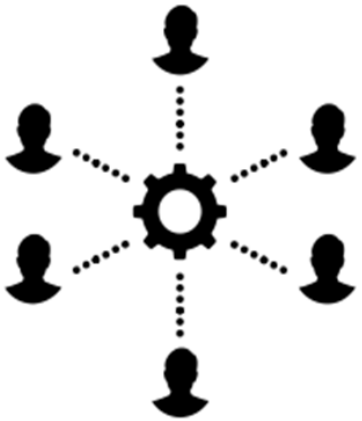
Cloud Security Maturity - Process for Assessment	
Phase 1	The scope of the project should be defined. Above all, it is important to identify the specific Use

Ciências ULisboa

Cloud Security
Readiness and Potential Risk assessment

Scope of the Assessment

Name of the author:	Luís Paulo Teixeira Ferreira
Date of the Assessment:	29/06/2017
Version:	V1
Organization:	FCUL
Department:	INFOSEC
Department Code:	DSI
Contact Name:	John Doe
Contact Email:	John.doe@fcul.com
Contact Phone:	965676673



Ciências ULisboa

Cloud Security Assessment - Criteria

Maturity Assessment

Not Performed	Performed Informally	Planned & Tracked	Well Defined	Quantitatively Controlled	Continuously Improving
There are no Security controls or plans in place. The required controls are **nonexistent**.	Base practices of the control area are generally performed on an **ad hoc basis**. There is general agreement within the organization that identified actions should be performed, and they are performed when required. The practices are not formally adopted, tracked, and reported on.	The base requirements for the control area are planned, implemented, and **repeatable**.	The primary distinction from "Planned & Tracked" is that in addition to being **repeatable** the processes used are more mature: **documented, approved, and implemented organization-wide.**	The primary distintion from "Well Defined is that the process is **measured and verified** (e.g. Auditable)	The primary distinction from "Quantitatively Controlled" is that the defined standard processes are **regularly reviewed and updated**. Improvements reflect an understanding of, and response to, a vulnerability's impact.

Higher the level -> Higher the **Cloud Security Maturity**

Potential Risk Factors - Impact

Impact Criteria

Impact	Description
Unavailability	The asset is unavailable and cannot be used or accessed by the organization. The cause can be accidental (failure of the CSP infrastructure), intentional (distributed Denial-of-Service [DDoS] attacks or legal (subpoena of database holding all data in a case of multitenancy architecture where one client's data are subject to legal investigation).
Loss	The asset is lost or destroyed. The cause can be accidental (natural disaster, wrong manipulation, etc.) or intentional (deliberate destruction of data).
Theft	The asset has been intentionally stolen and is now in possession of another individual/enterprise. Theft is a deliberate action that can involve data loss.
Disclosure	The asset has been released to unauthorized staff/enterprises or to the public.

Impact to asset type

Asset type	Unavailability	Loss	Theft	Disclosure
Data	Disruption of activities; Lack of resources to keep on with "business as usual"; possibility of data poisoning	Disruption of activities; required activation of backup restore procedures; possibility of partial loss of the asset (depending on the recovery point objective [RPO]); finantial loss associated with recovery efforts	Business competitive disadvantage; possibility of blackmail; loss of credibility with	Damage to company reputation or image; possibility of regulatory sanctions; financial impact
Applications/processes	Disruption of activities; Lack of resources to keep on with "business as usual"		Higher risk/threat of more selective attacks to data	

Ciências ULisboa

Cloud Security - Maturity Assessment

Filter by Security Domain

Author:	Luís Paulo Teixeira Ferreira	Organization:	FCUL	Contact Name:	John Doe
Date:	29/06/2017	Department:	INFOSEC	Contact Email:	John.doe@fcul.com
Version	V1	Dpt Code	DSI	Contact Phone:	965676673

Reset Evaluation

DOMAINS	SUBDOMAINS	SECTION	KEY PERFORMANCE INDICATOR (KPI)	MATURITY LEVEL Avg	MATURITY LEVEL Worst Case
Information Security Policies		1	Total Score for domain ->	Quantitatively Controlled	Performed Informally
Management direction for information security	Policies for information security	1.1.1	Does your institution have an information security policy considering the Cloud topic (policy and procedures in accordance with its use of cloud services) that has been approved by management?	Performed Informally	
			Has it been published and communicated to all relevant parties?	Continuously Improving	
	Review of the policies for information security	1.1.2	Does your institution review the Cloud policy at defined (and regular) intervals to encompass significant change and monitor for compliance?	Continuously Improving	
Organization of Information Security		2	Total Score for domain ->	Well Defined	Planned
Human Resource Security		3	Total Score for domain ->	Well Defined	Performed Informally
Asset Management		4	Total Score for domain ->	Continuously Improving	Planned
Access Control		5	Total Score for domain ->	Planned	Not Performed
Cryptography		6	Total Score for domain ->	Well Defined	Performed Informally
Physical and Environmental Security		7	Total Score for domain ->	Quantitatively Controlled	Quantitatively Controlled
Operations Security		8	Total Score for domain ->	Planned	Not Performed
Communications Security		9	Total Score for domain ->	Performed Informally	Not Performed
System acquisition, development and maintenance		10	Total Score for domain ->	Quantitatively Controlled	Performed Informally

Reset Evaluation

MATURITY LEVEL		TREND ANALYSIS		RATIONAL (e.g. Existing controls, process ID, applicable risks, etc)	POTENTIAL RISK FACTORS	ISO27017:2015 REFERENCE	CSA REFERENCE
Avg	Worst Case	Previous Assessment (avg)	Trend				
Quantitatively Controlled	Performed Informally	Well Defined	⇧				
Performed Informally		Performed Informally	⇨		R3, R15, R18	5.1.1	NA
Continuously Improving		Quantitatively Controlled	⇧				
Continuously Improving		Quantitatively Controlled	⇧		R1, R3, R18, R27, R38	5.1.2	
Well Defined	Planned	Planned	⇧				
Well Defined	Performed Informally	Not Performed	⇧				
Continuously Improving	Planned	Quantitatively Controlled	⇧				
Planned	Not Performed	Performed Informally	⇧				
Well Defined	Performed Informally	Quantitatively Controlled	⇩				
Quantitatively Controlled	Quantitatively Controlled	Continuously Improving	⇩				

Ciências ULisboa

Cloud Security - Potential Risk Factors

Author:	Luís Paulo Teixeira Ferreira	Organization:	FCUL	Contact Name:	John Doe
Date:	29/06/2017	Department:	INFOSEC	Contact Email:	John.doe@fcul.com
Version	V1	Dpt Code	DSI	Contact Phone:	965676673

RISK ID	CLOUD SERVICE MODELS			CLOUD-SPECIFIC RISK FACTORS	DESCRIPTION	CLOUD DEPLOYMENT MODELS				SOURCE	IMPACT CRITERIA AFFECTED
	IaaS	*PaaS*	*SaaS*			*Hybrid Cloud*	*Private Cloud*	*Public Cloud*	*Communitary Cloud*		
R1	X	X	X	**Legal transborder requirements**	CSPs are often transborder, and different countries have different legal requirements, especially concerning personal private information. The enterprise might be committing a violation of regulations in other countries when storing, processing or transmitting data within the CSP's infrastructure without the necessary compliance controls. Furthermore, government entities in the hosting country may require access to the enterprise's information with or without proper notification.	X		X	X	ISACA	Disclosure
					Customer data may be held in multiple jurisdictions, some of which may be high risk. If data centres are located in high-risk countries (e.g., those. lacking the rule of law and having an unpredictable legal framework and enforcement, autocratic police states, states that do not respect international agreements, etc), the corresponding sites where the data resides could be raided by local authorities and data or systems subject to enforced disclosure or seizure. Note that we are not implying here that all subpoena law-enforcement measures are unacceptable, merely that some may be so and that some legitimate seizures of hardware (which appear to be rare) may affect more customers than the targets of a law-enforcement action depending on how the data is stored.					ENISA	
R2	X	X	X	**Multitenancy and isolation failure**	One of the primary benefits of the cloud is the ability to perform dynamic allocation of physical resources when required. The most common approach is a multi-tenant environment (public cloud), where different entities share a pool of resources, including storage, hardware and network components. All resources allocated to a particular tenant should be "isolated" and protected to avoid disclosure of information to other tenants. For example, when allocated storage is no longer needed by a client it can be freely reallocated to another enterprise. In that case, sensitive data could be disclosed if the storage has not been scrubbed thoroughly (e.g., using forensic software).	X		X	X	ISACA	Theft, Disclosure
					Multi-tenancy and shared resources are two of the defining characteristics of cloud computing environments. Computing capacity, storage, and network are shared between multiple users. This class of risks includes the failure of mechanisms separating storage, memory, routing, and even reputation between different tenants of the shared infrastructure (e.g., so-called guest-hopping attacks, SQL injection attacks exposing multiple customers' data stored in the same table, and side channel attacks). Note that the likelihood (probability) of this incident scenario depends on the cloud model considered; it is likely to be low for private clouds and higher (medium) in the case of public clouds. The impact can be a loss of valuable or sensitive data, reputation damage and service interruption for cloud providers and their clients.					ENISA	

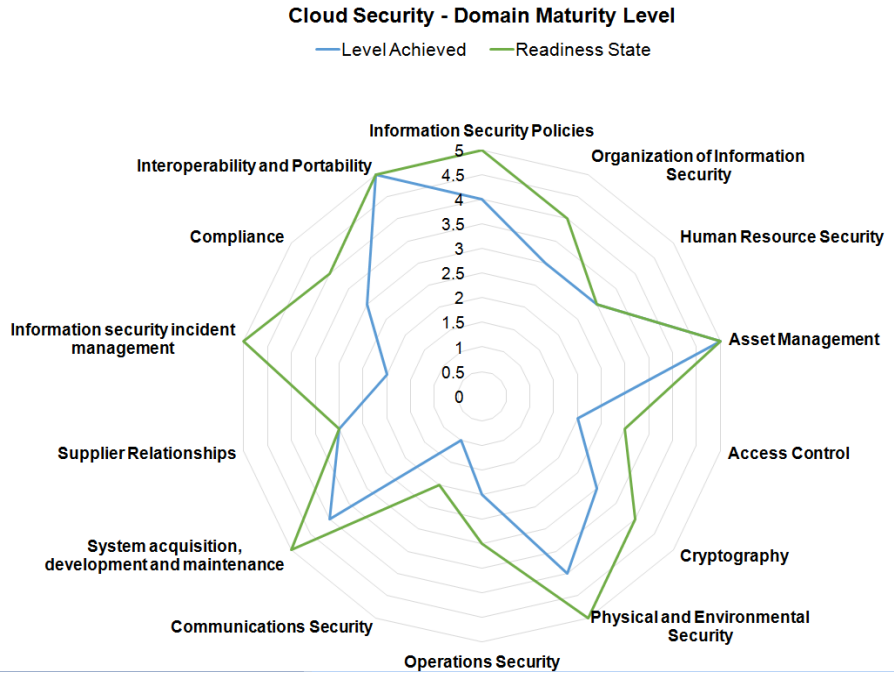
Ciências ULisboa

Executive Dashboard

Author:	Luís Paulo Teixeira	Organization:	FCUL	Contact	John Doe
Date:	29/06/2017	Department:	INFOSEC	Contact Email:	John.doe@siemens.com
Version:	V1	Dpt Code	DSI	Contact	910000000

Domain Maturity Level

Security Domain	Target Readiness State
Information Security Policies	Continuously Improving
Organization of Information Security	Quantitatively Controlled
Human Resource Security	Well Defined
Asset Management	Continuously Improving
Access Control	Well Defined
Cryptography	Quantitatively Controlled
Physical and Environmental Security	Continuously Improving
Operations Security	Well Defined
Communications Security	Planned
System acquisition, development and maintenance	Continuously Improving
Supplier Relationships	Well Defined
Information security incident management	Continuously Improving
Compliance	Quantitatively Controlled
Interoperability and Portability	Continuously Improving

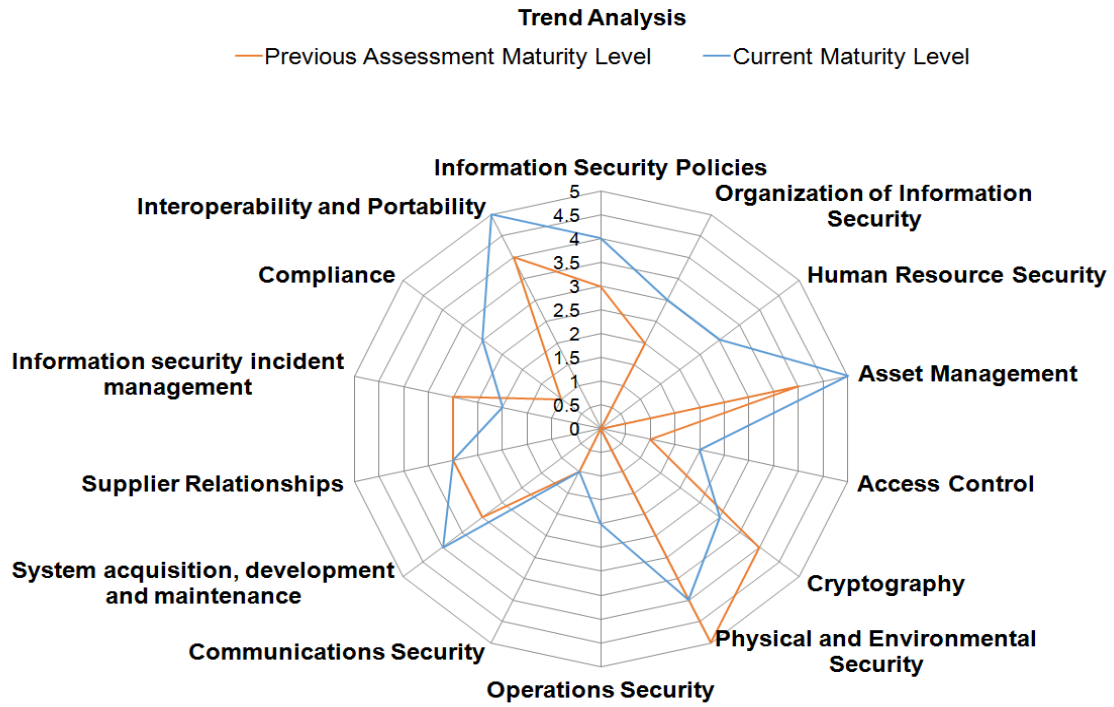


Ciências ULisboa

Executive Dashboard

Author:	Luís Paulo Teixeira	Organization:	FCUL	Contact	John Doe
Date:	29/06/2017	Department:	INFOSEC	Contact Email:	John.doe@siemens.com
Version:	V1	Dpt Code	DSI	Contact	910000000

Trend Analysis

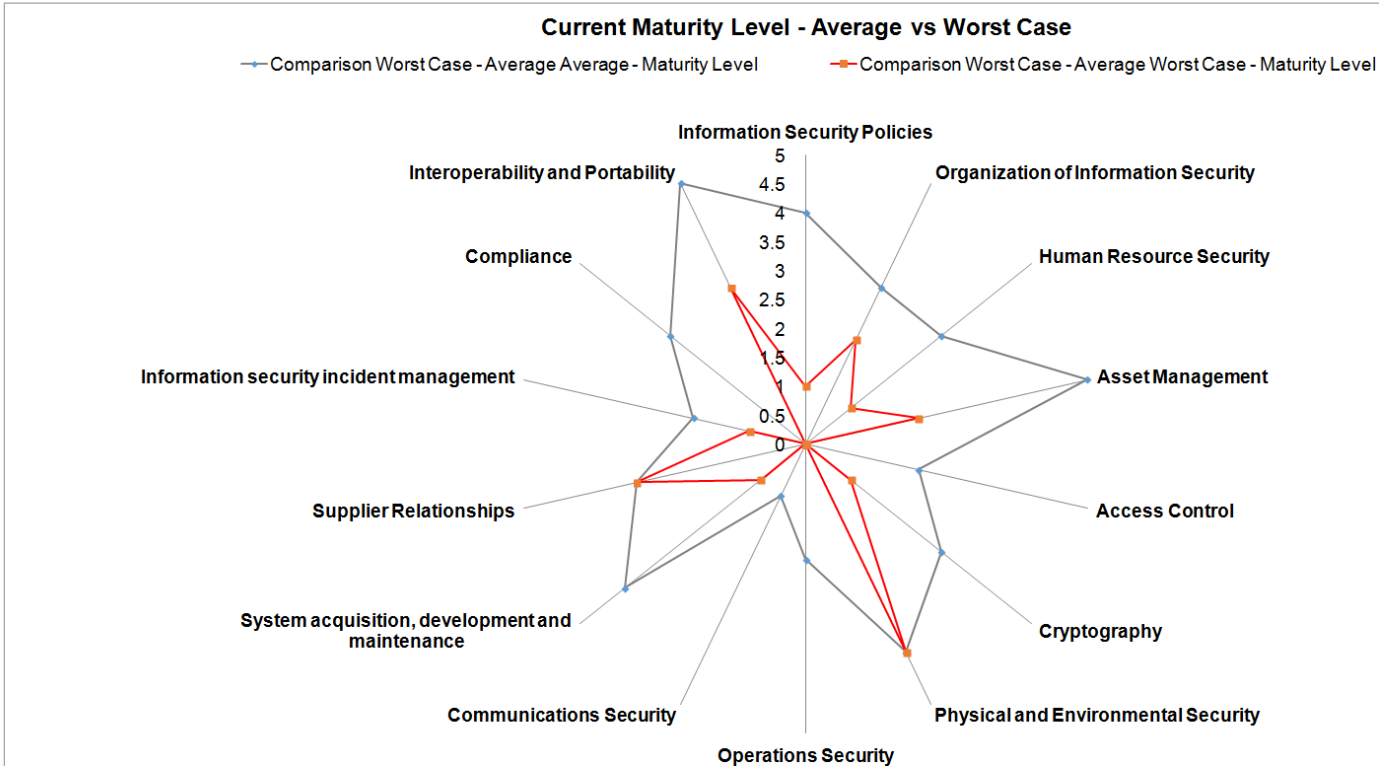


Ciências ULisboa

Executive Dashboard

Author:	Luis Paulo Teixeira	Organization:	FCUL	Contact	John Doe
Date:	29/06/2017	Department:	INFOSEC	Contact Email:	John.doe@siemens.com
Version:	V1	Dpt Code	DSI	Contact	910000000

Average vs Worst Case



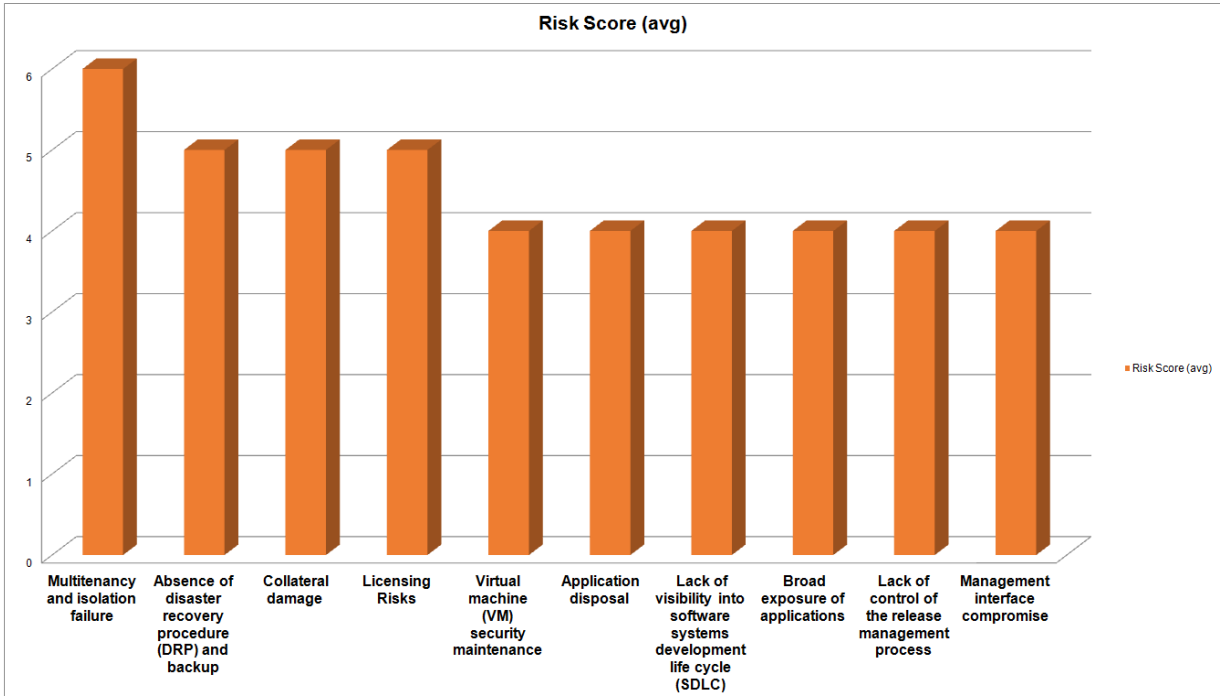
Ciências ULisboa

Cloud Security - Technical Dashboard

Author:	Luís Paulo Teixeira Ferreira	Organization:	FCUL	Contact Name:	John Doe
Date:	29/06/2017	Department:	INFOSEC	Contact Email:	John.doe@siemens.com
Version:	V1	Dpt Code	DSI	Contact Phone:	910000000

Top 10 Potential Risk Factors

Potential Risk Level	
Value	**Description**
1 and 2	Marginal
3	Minor
4	Moderate
5	Significant
6	Major



Ciências ULisboa

Cloud Security - Technical Dashboard

Author:	Luis Paulo Teixeira Ferreira	Organization:	FCUL	Contact Name:	John Doe
Date:	29/06/2017	Department:	INFOSEC	Contact Email:	John.doe@siemens.com
Version:	V1	Dpt Code	DSI	Contact Phone:	910000000

Top 10 Higher Risk Sub-Domains

Potential Risk Level	
Value	**Description**
1 and 2	Marginal
3	Minor
4	Moderate
5	Significant
6	Major

Ciências ULisboa

Cloud Security - Technical Dashboard

Author:	Luís Paulo Teixeira Ferreira	Organization:	FCUL	Contact Name:	John Doe
Date:	29/06/2017	Department:	INFOSEC	Contact Email:	John.doe@siemens.com
Version:	V1	Dpt Code	DSI	Contact Phone:	910000000

Cloud Deployment Models - Potential Risk

Potential Risk Level	
Value	**Description**
1 and 2	Marginal
3	Minor
4	Moderate
5	Significant
6	Major